Foundry EdgeIron User Guide



2100 Gold Street
P.O. Box 649100
San Jose, CA 95164-9100
Tel 408.586.1700
Fax 408.586.1900
www.foundrynetworks.com

May 2004

Copyright © 2004 Foundry Networks, Inc. All rights reserved.

No part of this work may be reproduced in any form or by any means – graphic, electronic or mechanical, including photocopying, recording, taping or storage in an information retrieval system – without prior written permission of the copyright owner.

The trademarks, logos and service marks ("Marks") displayed herein are the property of Foundry or other third parties. You are not permitted to use these Marks without the prior written consent of Foundry or such appropriate third party.

Foundry Networks, *EdgeIronEdgeIron*, *FastIron*, *IronView*, *JetCore*, *NetIron*, *ServerIron*, *TurboIron*, *IronWare*, *EdgeIron*, *IronPoint*, the Iron family of marks and the Foundry Logo are trademarks or registered trademarks of Foundry Networks, Inc. in the United States and other countries.

All other trademarks mentioned in this document are the property of their respective owners.

Contents

Chapter 1.
About This Guide 1-1
Audience 1-1
Nomenclature 1-1
How to Get Help 1-1
Foundry Networks Technical Support 1-1
Web Access 1-1
E-mail Access 1-1
Telephone Access 1-2
Warranty Coverage 1-2
Related Publications 1-2
Summary of Features 1-2
What's New In This Release 1-2
Technical Specifications 1-3
List of Features 1-3

Chapter 2.
Switch Management 2-1
Connecting to the Switch 2-1
Configuration Options 2-1
Required Connections 2-2
Remote Connections 2-3
Basic Configuration 2-3
Console Connection 2-3
Setting Passwords 2-4
Setting an IP Address 2-4
Manual Configuration 2-4
Dynamic Configuration 2-5

 © 2004 Foundry Networks, Inc.

Enabling SNMP Management Access 2-6
Community Strings 2-6
Trap Receivers 2-7
Saving Configuration Settings 2-7
Managing System Files 2-8
System Defaults 2-9

Chapter 3.
Configuring the Switch 3-1
Using the Web Interface 3-1
Navigating the Web Browser Interface 3-2
Home Page 3-2
Configuration Options 3-2
Panel Display 3-3
Main Menu 3-3
Basic Configuration 3-6
Displaying System Information 3-6
Displaying Switch Hardware/Software Versions 3-7
Displaying Bridge Extension Capabilities 3-8
Setting the IP Address 3-10
Manual Configuration 3-11
Using DHCP/BOOTP 3-11
Managing Firmware 3-12
Downloading System Software from a Server 3-12
Saving or Restoring Configuration Settings 3-13
Copying the Running Configuration to a File 3-15
System Logs 3-15
System Logs Configuration 3-16
Remote Logs Configuration 3-17
Sending Simple Mail Transfer Protocol Alerts 3-18
Resetting the System 3-20
Configuring SNTP 3-20
Setting the Time Zone 3-22
Configuring SNMP 3-22
Setting Community Access Strings 3-22
Access Mode 3-23
Specifying Trap Managers 3-23
Security 3-24
Configuring the Logon Password 3-24
Configuring RADIUS/TACACS Logon Authentication 3-25
HTTPS 3-27
SSH 3-28
Generating the Host Key Pair 3-30
Configuring the SSH Server 3-31

 © 2004 Foundry Networks, Inc.

Configuring Port Security 3-32
Configuring 802.1x Port Authentication 3-34
Configuring 802.1x Global Settings 3-36
Configuring Port Authorization Mode 3-37
Displaying 802.1x Statistics 3-38
Access Control Lists 3-40
Configuring Access Control Lists 3-40
Setting the ACL Name and Type 3-41
Configuring a Standard IP ACL 3-41
Configuring an Extended IP ACL 3-42
Configuring a MAC ACL 3-44
Configuring ACL Masks 3-46
Specifying the Mask Type 3-46
Configuring an IP ACL Mask 3-47
Configuring a MAC ACL Mask 3-48
Binding a Port to an Access Control List 3-49
Filtering IP Addresses for Management Access 3-51
Port Configuration 3-52
Displaying Connection Status 3-52
Configuring Interface Connections 3-54
Statically Configuring a Trunk 3-55
Dynamically Configuring a Trunk 3-56
Enabling LACP on Selected Ports 3-57
Configuring LACP Parameters 3-58
Dynamically Creating a Port Channel 3-58
Displaying LACP Port Counters 3-60
Counter Information 3-60
Displaying LACP Settings and Status for the Local Side 3-61
Internal Configuration Information 3-61
Displaying LACP Settings and Status for the Remote Side 3-63
Neighbor Configuration Information 3-63
Setting Broadcast Storm Thresholds 3-64
Configuring Port Mirroring 3-66
Configuring Rate Limits 3-67
Address Table Settings 3-69
Setting Static Addresses 3-69
Displaying the Address Table 3-70
Changing the Aging Time 3-71
Spanning Tree Protocol 3-72
Enabling a Single Instance of STP per VLAN on an EdgeIron 3-73
STP Information 3-74
STP Configuration 3-77
STP Port and Trunk Information 3-81
STP Port and Trunk Configuration 3-83
Multiple Spanning Tree Protocol Configuration 3-85
Displaying Interface Settings for MSTP 3-87
Configuring Interface Settings for MSTP 3-89

 © 2004 Foundry Networks, Inc.

VLAN Configuration 3-90
Assigning Ports to VLANs 3-90
Forwarding Tagged/Untagged Frames 3-91
Enabling or Disabling GVRP (Global Setting) 3-92
Displaying Basic VLAN Information 3-92
Displaying Current VLANs 3-93
Creating VLANs 3-95
Adding Interfaces Based on Membership Type 3-96
Adding Interfaces Based on Static Membership 3-98
Configuring VLAN Behavior for Interfaces 3-98
Configuring Private VLANs 3-101
Enabling Private VLANs 3-101
Configuring Uplink and Downlink Ports 3-101
Priority Configuration 3-102
Setting the Default Priority for Interfaces 3-102
Mapping CoS Values to Egress Queues 3-103
Setting the Service Weight for Traffic Classes 3-105
Mapping Layer 3/4 Priorities to CoS Values 3-106
Selecting IP Precedence/DSCP Priority 3-107
Mapping IP Precedence 3-107
Mapping DSCP Priority 3-109
Mapping IP Port Priority 3-110
Mapping CoS Values to ACLs 3-112
Changing Priorities Based on ACL Rules 3-113
Multicast Configuration 3-114
Configuring IGMP Parameters 3-115
Interfaces Attached to a Multicast Router 3-116
Displaying Interfaces Attached to a Multicast Router 3-116
Specifying Interfaces Attached to a Multicast Router 3-117
Displaying Port Members of Multicast Services 3-118
Adding Multicast Addresses to VLANs 3-119
Showing Device Statistics 3-120

Chapter 4.
Command Line Interface 4-1
Using the Command Line Interface 4-1
Accessing the CLI 4-1
Console Connection 4-1
Telnet Connection 4-1
Entering Commands 4-2
Keywords and Arguments 4-2
Minimum Abbreviation 4-3

 © 2004 Foundry Networks, Inc.

Command Completion 4-3
Getting Help on Commands 4-3
Showing Commands 4-3
Partial Keyword Lookup 4-4
Negating the Effect of Commands 4-4
Using Command History 4-5
Understanding Command Modes 4-5
Exec Commands 4-5
Configuration Commands 4-6
Command Line Processing 4-7
Command Groups 4-7
General Commands 4-8
enable 4-9
disable 4-9
configure 4-10
show history 4-10
reload 4-11
prompt 4-12
end 4-12
exit 4-12
quit 4-13
Flash/File Commands 4-13
copy 4-14
delete 4-15
dir 4-16
whichboot 4-16
boot system 4-17
System Management Commands 4-18
hostname 4-20
username 4-20
enable password 4-21
management 4-22
show management 4-23
jumbo frame 4-23
light unit 4-24
ip http port 4-24
ip http server 4-25
ip http secure-server 4-25
ip http secure-port 4-26
Secure Shell Commands 4-27
ip ssh server 4-29
ip ssh timeout 4-29
ip ssh authentication-retries 4-30
ip ssh server-key size 4-30
delete public-key 4-31
ip ssh crypto host-key generate 4-31
ip ssh crypto zeroize 4-32

 © 2004 Foundry Networks, Inc.

ip ssh save host-key 4-32
show ip ssh 4-33
show ssh 4-33
show public-key 4-34
ip ssh 4-35
ip ssh server 4-35
disconnect ssh 4-36
show ssh 4-36
show ip ssh 4-37
Event Logging Commands 4-37
logging on 4-37
logging history 4-38
logging host 4-39
logging facility 4-39
logging trap 4-40
clear logging 4-41
show log 4-41
show logging 4-42
System Status Commands 4-43
show startup-config 4-43
show running-config 4-44
show system 4-46
show users 4-47
show version 4-48
SMTP Alert Commands 4-48
logging sendmail host 4-48
logging sendmail level 4-49
logging sendmail source-email 4-50
logging sendmail destination-email 4-50
logging sendmail 4-50
show logging sendmail 4-51
Time Commands 4-51
sntp client 4-52
sntp server 4-52
sntp poll 4-53
sntp broadcast client 4-53
show sntp 4-54
clock timezone 4-54
calendar set 4-55
show calendar 4-55
Authentication Commands 4-56
authentication login 4-57
authentication enable 4-58
radius-server host 4-58
radius-server port 4-59
radius-server key 4-59
radius-server retransmit 4-60
radius-server timeout 4-60
show radius-server 4-60
tacacs-server host 4-61
tacacs-server port 4-61
tacacs-server key 4-62
show tacacs-server 4-62
authentication dot1x default 4-62
dot1x default 4-63

 © 2004 Foundry Networks, Inc.

dot1x max-req 4-63
dot1x port-control 4-63
dot1x re-authenticate 4-64
dot1x re-authentication 4-64
dot1x timeout quiet-period 4-64
dot1x timeout re-authperiod 4-65
dot1x timeout tx-period 4-65
show dot1x 4-66

Access Control List Commands 4-67

IP ACLs 4-69

access-list ip 4-70
permit, deny (Standard ACL) 4-70
permit, deny (Extended ACL) 4-71
show ip access-list 4-73
access-list ip mask-precedence 4-73
mask (IP ACL) 4-74
show access-list ip mask-precedence 4-76
ip access-group 4-77
show ip access-group 4-77
map access-list ip 4-78
show map access-list ip 4-79
match access-list ip 4-79
show marking 4-80

MAC ACLs 4-80

access-list mac 4-81
permit, deny (MAC ACL) 4-81
show mac access-list 4-83
access-list mac mask-precedence 4-83
mask (MAC ACL) 4-84
show access-list mac mask-precedence 4-85
permit offset, deny offset (MAC ACL) 4-86
mac access-group 4-87
show mac access-group 4-87
map access-list mac 4-88
show map access-list mac 4-89
match access-list mac 4-89

ACL Information 4-90

show access-list 4-90
show access-group 4-90

SNMP Commands 4-91

snmp-server community 4-91
snmp-server contact 4-92
snmp-server location 4-92
snmp-server host 4-93
snmp-server enable traps 4-94
snmp ip filter 4-94
show snmp 4-95

IP Commands 4-96

ip address 4-97
ip dhcp restart 4-98
ip default-gateway 4-98
show ip interface 4-99
show ip redirects 4-99
ping 4-100

 © 2004 Foundry Networks, Inc.

Line Commands 4-101
line 4-101
login 4-102
password 4-103
exec-timeout 4-103
password-thresh 4-104
silent-time 4-105
databits 4-105
parity 4-106
speed 4-106
stopbits 4-107
show line 4-107
Interface Commands 4-108
interface 4-109
description 4-109
speed-duplex 4-110
negotiation 4-110
capabilities 4-111
flowcontrol 4-112
shutdown 4-113
switchport broadcast 4-114
port security 4-114
port security (EdgeIron 2402CF) 4-116
clear counters 4-117
show interfaces status 4-117
show interfaces counters 4-118
show interfaces switchport 4-119
Address Table Commands 4-121
mac-address-table static 4-121
show mac-address-table 4-122
clear mac-address-table dynamic 4-123
mac-address-table aging-time 4-123
show mac-address-table aging-time 4-123
Spanning Tree Commands 4-124
spanning-tree 4-125
spanning-tree forward-time 4-126
spanning-tree hello-time 4-126
spanning-tree max-age 4-127
spanning-tree priority 4-127
spanning-tree pathcost method 4-128
spanning-tree transmission-limit 4-128
spanning-tree spanning-disabled 4-129
Multiple Spanning Tree 4-129
spanning-tree mst-configuration 4-129
spanning-tree mst-configuration 4-130
mst vlan 4-130
mst priority 4-131
name 4-131
revision 4-132
max-hops 4-132
spanning-tree cost 4-133
spanning-tree port-priority 4-134
spanning-tree portfast 4-134
spanning-tree edge-port 4-135
spanning-tree protocol-migration 4-136
spanning-tree link-type 4-136

 © 2004 Foundry Networks, Inc.

spanning-tree mst cost 4-137
spanning-tree mst port-priority 4-138
show spanning-tree 4-138
show spanning-tree mst configuration 4-139
VLAN Commands 4-140
vlan 4-141
untagged ethernet 4-142
tagged ethernet 4-142
dual-mode 4-143
Configuring VLAN Interfaces 4-144
interface vlan 4-144
switchport mode 4-144
switchport acceptable-frame-types 4-145
switchport ingress-filtering 4-145
switchport native vlan 4-146
switchport allowed vlan 4-147
switchport forbidden vlan 4-148
show vlan 4-148
Private VLAN Commands 4-149
Editing Private VLAN Groups 4-150
private-vlan 4-150
private vlan association 4-150
Configuring Private VLAN Interfaces 4-151
switchport mode private-vlan 4-151
switchport private-vlan host-association 4-152
switchport private-vlan mapping 4-152
Displaying Private VLAN Information 4-153
show vlan private-vlan 4-153
GVRP and Bridge Extension Commands 4-153
switchport gvrp 4-154
show gvrp configuration 4-154
garp timer 4-155
show garp timer 4-156
bridge-ext gvrp 4-156
show bridge-ext 4-157
IGMP Snooping Commands 4-157
Basic IGMP Commands 4-158
ip igmp snooping 4-158
ip igmp snooping vlan static 4-158
ip igmp snooping version 4-159
show ip igmp snooping 4-159
show mac-address-table multicast 4-160
IGMP Querier Commands 4-160
ip igmp snooping querier 4-160
ip igmp snooping query-count 4-161
ip igmp snooping query-interval 4-161
ip igmp snooping query-max-response-time 4-162
ip igmp snooping router-port-expire-time 4-163
Multicast Router Commands 4-163
ip igmp snooping vlan mrouter 4-163
show ip igmp snooping mrouter 4-164

 © 2004 Foundry Networks, Inc.

Priority Commands 4-164
Layer 2 Priority Commands 4-165
switchport priority default 4-165
queue bandwidth 4-166
queue cos-map 4-167
show queue bandwidth 4-168
show queue cos-map 4-168
Layer 3 and 4 Priority Commands 4-169
map ip precedence (Global Configuration) 4-169
map ip precedence (Interface Configuration) 4-169
map ip dscp (Global Configuration) 4-170
map ip dscp (Interface Configuration) 4-171
map ip port (Global Configuration) 4-172
map ip port (Interface Configuration) 4-172
show map ip precedence 4-173
show map ip dscp 4-173
show map ip port 4-174
Mirror Port Commands 4-175
port monitor 4-175
show port monitor 4-176
Port Trunking Commands 4-177
channel-group 4-178
Dynamic Trunk Configuration Commands 4-178
lacp 4-178
lacp system-priority 4-179
lacp admin-key (Ethernet Interface) 4-180
lacp admin-key (Port Channel) 4-181
lacp port-priority 4-181
show lacp 4-182
Rate Limiting Commands 4-186
rate-limit 4-186

Appendix A.
Using Syslog A-1
Overview A-1
Displaying Syslog Messages A-2
Configuring the Syslog Service A-2
Displaying the Syslog Configuration A-2
Flash and RAM Buffers A-3
Time Stamps A-4
Example of Syslog Messages on a Device Whose Onboard Clock Is Set A-5
Displaying and Configuring Syslog Buffer Parameters Using the Web Management Interface A-5
Disabling or Re-Enabling Syslog A-6
Specifying a Syslog Server A-6
Using The Web Management Interface A-7
Specifying an Additional Syslog Server A-7
Changing the Log Facility A-7
Clearing the Syslog Messages from the Local Buffer A-7

 © 2004 Foundry Networks, Inc.

Syslog Messages A-8

Appendix B.
Troubleshooting B-1

Troubleshooting Chart B-1

Appendix C.
Upgrading Firmware via the Serial Port C-1

Appendix D.
Pin Assignments D-1

Console Port Pin Assignments D-1

DB-9 Port Pin Assignments D-1

Console Port to 9-Pin DTE Port on PC D-1

Console Port to 25-Pin DTE Port on PC D-2

Glossary

Index

 © 2004 Foundry Networks, Inc.

 © 2004 Foundry Networks, Inc.

Chapter 1
About This Guide

Audience

This guide is for system administrators with a working knowledge of network management.

You should be familiar with switching and networking concepts.

Nomenclature

This guide uses the following typographical conventions to show information:

`Monospace font` – Enter text exactly as it appears in this guide.

Note: emphasizes an important fact or calls your attention to a dependency.

How to Get Help

If you need assistance, Foundry Networks is committed to ensuring that your investment in our products remains cost-effective by offering a variety of support options.

Foundry Networks Technical Support

Foundry Networks technical support will ensure that the fast and easy access that you have come to expect from your Foundry Networks products will be maintained.

Web Access

Point your browser to the following URL: http://www.foundrynetworks.com.

Navigate to Services/Technical Support.

Click the Login button, then enter your user name and password to gain access to the Foundry support site.

E-mail Access

Technical requests can also be sent to the e-mail address: **support@foundrynet.com**

© 2004 Foundry Networks, Inc.

Telephone Access

- 1.877.TURBOCALL (887.2622): United States
- 1.408.586.1881: Outside the United States

Warranty Coverage

Contact Foundry Networks using any of the methods listed above for information about the standard and extended warranties.

Related Publications

Refer to the *Foundry EdgeIron 24G-A and 24G Installation Guide*, *Foundry EdgeIron 4802CF Installation Guide, Foundry EdgeIron 48G Installation Guide, or Foundry EdgeIron 2402CF Installation Guide* for instructions on how to install the switch, and refer to the *Foundry EdgeIron External Redundant Power Supply* for instructions on connecting an external redundant power supply to an EdgeIron switch.

Summary of Features

This manual contains the configuration and management commands for the EdgeIron products. It contains specific firmware information for the EdgeIron 24G-A, EdgeIron 24G, EdgeIron 4802CF, EdgeIron 48G, and EdgeIron 2402CF Layer 2 switches. It provides information for features in the following software versions:

- EdgeIron 2402CF: software release version 2.2.4.11
- EdgeIron 4802CF: software release version 2.2.4.11
- EdgeIron 48G: software release version 2.2.4.11
- EdgeIron 24G-A: software release version 2.2.4.11
- EdgeIron 24G: software release version 2.0.1.9

What's New In This Release

The following features are new in this release:

Feature	Discussed In the Following Sections
Foundry per VLAN Spanning Tree support	"Spanning Tree Protocol" on page 3-72
Addition of "vlan" command	See "vlan" on page 4-141.
Additon of "untagged ethernet" command	See "untagged ethernet" on page 4-142.
Addition of "tagged ethernet" command	See "tagged ethernet" on page 4-142.
Addition of "dual-mode" command	See "dual-mode" on page 4-143.

© 2004 Foundry Networks, Inc.

Technical Specifications

The following table summarizes the technical specifications for the switches:

Properties	EdgeIron 2402CF	EdgeIron 4802CF	EdgeIron 24G	EdgeIron 24G-A	EdgeIron 48G
10/100 Base-T Ports	24	48	0	0	0
10/100/1000 Base-T ports	2	2	24	24	44
Mini-GBIC slots	2	2	4	4	4
Switching Performance (Gbps)	8.8	13.6	48	48	80
Forwarding Rate for a 64-byte packet (Mpps)	6.6	10.2	35.7	35.7	60
Maximum Number of MAC Addresses	8,000	8,000	16,000	16,000	16,000
Physical Dimensions (HxWxD)	1.7”x17.37”x9” (4.3x44x22.8 cm)	1.7”x17.37”x12.76” (4.3x44x32.4 cm)	1.7”x17.37”x13.9” (4.3x44x35.3 cm)	1.7"x17.37"x13.9 (4.3x44x35.3 cm)	1.17"x17.37"x13.9" (4.3x44x35.3 cm)
Weight	7 lbs (3.18 kg)	9.5 lbs (4.36 kg)	9.5 lbs (4.36 kg)	9.5 lbs (4.36 kg)	12.9lbs (5.86 kg)
Power Consumption (Watt)	60W maximum	60W maximum	100W maximum	100W maximum	100W maximum

List of Features

The following table summarizes the features available in the switches. Refer to the appropriate sections in this manual for any feature limitations.

Features	EdgeIron 2402CF	EdgeIron 4802CF	EdgeIron 24G	EdgeIron 24G-A	EdgeIron 48G
System					
Software	Version 2.2.4.7	Version 2.2.4.7	Version 2.0.1.9	Version 2.2.4.7	Version 2.2.4.7
Size	1U	1U	1U	1U	1U
Uplink	mGBIC/TX Combo	mGBIC/TX Combo	mGBIC/TX Combo	mGBIC/TX Combo	mGBIC/TX Combo
Redundant Power	External	External	External	External	External
Jumbo Frames	No	No	Yes (up to 9 Kbytes)	Yes (up to 9 Kbytes)	Yes (up to 9 Kbytes)
Flash Memory	8 Mbytes	8 Mbytes	4 Mbytes	8 Mbytes	8 Mbytes
DRAM	32 Mbytes	32 Mbytes	16 Mbytes	32 Mbytes	32 Mbytes
SNTP	Yes	Yes	No	Yes	Yes
ARP	Yes	Yes	Yes	Yes	Yes

© 2004 Foundry Networks, Inc.

Features	EdgeIron 2402CF	EdgeIron 4802CF	EdgeIron 24G	EdgeIron 24G-A	EdgeIron 48G
IP Address Management					
BootP	Yes	Yes	Yes	Yes	Yes
DHCP Clients	Yes	Yes	Yes	Yes	Yes
Configuration Management	Yes	Yes	Yes	Yes	Yes
Security					
RADIUS and TACAC+ authentication	Yes	Yes	Yes	Yes	Yes
TFTP	Yes	Yes	Yes	Yes	Yes
Remote Logging	Yes	Yes	Yes	Yes	Yes
HTTPS	Yes	Yes	Yes	Yes	Yes
SSH (version 2.0)	Yes	Yes	No	Yes	Yes
SSH (version 1.5)	Yes	Yes	Yes	Yes	Yes
SNMP (v1 and v2c)	Yes	Yes	Yes	Yes	Yes
Port Security	Yes	Yes	Yes	Yes	Yes
IEEE 802.1x	Yes	Yes	No	Yes	Yes
Layer 2 – VLANs					
IEEE 802.1q Port-based VLANs	Yes	Yes	Yes	Yes	Yes
VLANs per switch	255	255	255	255	255
Private VLANs	Yes	Yes	No	Yes	Yes
Dual-mode*	Yes	Yes	Yes	Yes	Yes
GVRP	Yes	Yes	Yes	Yes	Yes
IEEE 802.1v	No	No	No	No	No
Foundry Per VLAN STP compatible	Yes	Yes	No	Yes	Yes
Layer 2 – Spanning Tree					
IEEE 802.1D (STP)	Yes	Yes	Yes	Yes	Yes
Fast Link Option	Yes	Yes	Yes	Yes	Yes
IEEE 802.1s (MSTP)	Yes	Yes	No	Yes	Yes
IEEE 802.1W (RSTP)	Yes	Yes	Yes	Yes	Yes
Layer 2 – Priority					
Priority (IEEE 802.1p & IEEE 802.1q)	Yes	Yes	Yes	Yes	Yes
Priority queues per port	4	4	4	8	8
IP Precedence, IP DSCP, IP Port	Yes	Yes	Yes	Yes	Yes

© 2004 Foundry Networks, Inc.

Features	EdgeIron 2402CF	EdgeIron 4802CF	EdgeIron 24G	EdgeIron 24G-A	EdgeIron 48G
Strict scheduling for priority queue	Yes	Yes	No	Yes	Yes
Layer 2 – Priority/QoS					
L2: 802.1p - Tag-based	Yes	Yes	Yes	Yes	Yes
L2: 802.1p - Port-based	Yes	Yes	Yes	Yes	Yes
L2: 802.1p - Queuing	4 queues per port	4 queues per port	4 queues per port	8 queues per port	8 queues per port
L3 Aware: DiffServ/ IP TOS	Yes	Yes	Yes	Yes	Yes
L4 Aware: TCP port-based	No	Yes	No	No	No
Layer 2 – Link Aggregation					
802.3ad	Yes	Yes	Yes	Yes	Yes
Cisco EhterChannel	Yes	Yes	Yes	Yes	Yes
Layer 2 – Port Mirroring	Yes	Yes	Yes	Yes	Yes
Layer 2 – Trunking					
10/100 Trunks	Yes	Yes	Yes	Yes	Yes
Gigabit Trunks	Yes	Yes	Yes	Yes	Yes
IEEE 802.3ad	Yes	Yes	Yes	Yes	Yes
Layer 2 – Rate Limiting	Yes	Yes	No	Yes	Yes
Layer 2 – Access Control Lists 128 rules per port	No Management IP Filter only		No	Yes Management Pass through	
Management Interface Access Filtering	Yes	Yes	No	Yes	Yes
IEEE 802.3x	Yes	Yes	Yes	Yes	Yes
Layer 3 – ToS/DSCP Honoring	Yes	Yes	Yes	Yes	Yes
Multicast					
IGMP Snooping	Yes	Yes	Yes	Yes	Yes
Broadcast storm control	Yes	Yes	Yes	Yes	Yes
MIB Support					
MIB II	Yes	Yes	Yes	Yes	Yes
Bridging MIB	Yes	Yes	Yes	Yes	Yes
Interface MIB	Yes	Yes	Yes	Yes	Yes
RMON MIB	Yes	Yes	Yes	Yes	Yes
RADIUS MIB	Yes	Yes	Yes	Yes	Yes
Ethernet-like MIB	Yes	Yes	Yes	Yes	Yes
Entity MIB	Yes	Yes	Yes	Yes	Yes

© 2004 Foundry Networks, Inc.

Features	EdgeIron 2402CF	EdgeIron 4802CF	EdgeIron 24G	EdgeIron 24G-A	EdgeIron 48G
Extended MIB	Yes	Yes	Yes	Yes	Yes
SNMP MIB	Yes	Yes	Yes	Yes	Yes

* Dual Mode refers to a port that can support both tagged and untagged VLANs.

© 2004 Foundry Networks, Inc.

Chapter 2
Switch Management

Connecting to the Switch

Configuration Options

The Foundry EdgeIron switches include a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON and a Web-based interface. A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI).

Note: The IP address for this switch is assigned via DHCP by default. To change this address, see on page 2-4.

The switch's HTTP Web agent allows you to configure switch parameters, monitor port connections, and display statistics graphically using a standard Web browser such as Netscape Navigator version 6.2 and higher or Microsoft IE version 5.0 and higher. The switch's Web management interface can be accessed from any computer attached to the network.

The switch's management agent is based on SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using management software.

The CLI program can be accessed by a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet connection over the network.

The switch's CLI configuration program, Web interface, and SNMP agent allow you to perform the following management functions:

- Set user names and passwords for up to 16 users
- Set an IP interface for a management VLAN
- Configure SNMP parameters
- Enable/disable any port
- Set the speed/duplex mode for any port
- Configure up to 255 IEEE 802.1Q VLANs

© 2004 Foundry Networks, Inc.

- Enable GVRP automatic VLAN registration
- Configure IGMP multicast filtering
- Upload and download of system firmware via TFTP
- Upload and download of switch configuration files via TFTP
- Configure spanning tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure up to six static or LACP trunks
- Enable port mirroring
- Set broadcast storm control on any port
- Display system information and statistics

Required Connections

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch. A null-modem console cable is provided with the switch.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable.

To connect a terminal to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the RS-232 serial port on the switch.
3. Make sure the terminal emulation software is set as follows:
   - Select the appropriate serial port (COM port 1 or COM port 2).
   - Set the data rate to 9600 baud.
   - Set the data format to 8 data bits, 1 stop bit, and no parity.
   - Set flow control to none.
   - Set the emulation mode to VT100.
   - When using HyperTerminal, select Terminal keys, not Windows keys.

Note: When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

4. Once you have set up the terminal correctly, the console login screen will be displayed.

Note: Refer to on page 4-101 for a complete description of console configuration options.

 © 2004 Foundry Networks, Inc.

For a description of how to use the CLI, see on page 4-1. For a list of all the CLI commands and detailed information on using the CLI, refer to on page 4-7.

Remote Connections

Prior to accessing the switch's onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using a console connection, DHCP or BOOTP protocol.

The IP address for this switch is assigned via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP or BOOTP, see "Setting an IP Address" on page 2-4.

Note: This switch supports four concurrent Telnet sessions.

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program can be accessed using Telnet from any computer attached to the network. The switch can also be managed by any computer using a Web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above), or from a network computer using network management software.

Note: The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

Basic Configuration

Console Connection

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of those available at the Privileged Exec level and allow you to only display information and use basic utilities. To fully configure switch parameters, you must access the CLI at the Privileged Exec level.

Access to both CLI levels are controlled by user names and passwords. The switch has a default user name and password for each level. To log into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate your console connection, press <Enter>. The “User Access Verification” procedure starts.
2. At the Username prompt, enter “admin.”
3. At the Password prompt, also enter “admin.” (The password characters are not displayed on the console screen.)
4. The session is opened and the CLI displays the “Console#” prompt indicating you have access at the Privileged Exec level.

 © 2004 Foundry Networks, Inc.

Setting Passwords

Note: If this is your first time to log into the CLI program, you should define new passwords for both default user names using the “username” command, record them and put them in a safe place.

Passwords can consist of up to eight alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface with the default user name and password “admin” to access the Privileged Exec level.
2. Type “configure” and press <Enter>.
3. Type “username guest password 0 *password*,” for the Normal Exec level, where *password* is your new password. Press <Enter>.
4. Type “username admin password 0 *password*,” for the Privileged Exec level, where *password* is your new password. Press <Enter>.

```
Username: admin
Password:
CLI session with the EdgeIron 4802CF is opened.
To end the CLI session, enter [Exit].
Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#
```

Setting an IP Address

You must establish IP address information for the switch to obtain management access through the network. This can be done in either of the following ways:

Manual – You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router.

Dynamic – The switch sends IP configuration requests to BOOTP or DHCP address allocation servers on the network.

Note: Only one VLAN interface can be assigned an IP address (the default is VLAN 1). This defines the management VLAN, the only VLAN through which you can gain management access to the switch. If you assign an IP address to any other VLAN, the new IP address overrides the original IP address and this becomes the new management VLAN.

Manual Configuration

You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

 © 2004 Foundry Networks, Inc.

Note: The IP address for this switch is assigned via DHCP by default.

Before you can assign an IP address to the switch, you must obtain the following information from your network administrator:

- IP address for the switch
- Default gateway for the network
- Network mask for this network

To assign an IP address to the switch, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. Type “ip address *ip-address netmask*,” where “ip-address” is the switch IP address and “netmask” is the network mask for the network. Press <Enter>.
3. Type “exit” to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the default gateway for the network to which the switch belongs, type “ip default-gateway *gateway*,” where “gateway” is the IP address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5
   255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
Console(config)#
```

Dynamic Configuration

If you select the “bootp” or “dhcp” option, IP will be enabled but will not function until a BOOTP or DHCP reply has been received. You therefore need to use the “ip dhcp restart” command to start broadcasting service requests. Requests will be sent periodically in an effort to obtain IP configuration information. (BOOTP and DHCP values can include the IP address, subnet mask, and default gateway.)

If the “bootp” or “dhcp” option is saved to the startup-config file, then the switch will start broadcasting service requests as soon as it is powered on.

To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. At the interface-configuration mode prompt, use one of the following commands:
   - To obtain IP settings through DHCP, type “ip address dhcp” and press <Enter>.
   - To obtain IP settings through BOOTP, type “ip address bootp” and press <Enter>.

 © 2004 Foundry Networks, Inc.

3. Type “exit” to return to the global configuration mode. Press <Enter>.
4. Type “ip dhcp restart” to begin broadcasting service requests. Press <Enter>.
5. Wait a few minutes, and then check the IP configuration settings, by typing the “show ip interface” command. Press <Enter>.
6. Then save your configuration changes by typing “copy running-config startup-config.” Enter the startup file name and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart
Console#show ip interface
IP interface vlan
 IP address and netmask: 10.1.0.54 255.255.255.0 on
   VLAN 1,and address mode: User specified.
Console#copy running-config startup-config
Startup configuration file name []: startup

Console#
```

Enabling SNMP Management Access

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications. You can configure the switch to (1) respond to SNMP requests or (2) generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

Community Strings

Community strings are used to control management access to SNMP stations, as well as to authorize SNMP stations to receive trap messages from the switch. You therefore need to assign community strings to specified users or user groups, and set the access level.

The default strings are:

- **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - with read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Note: If you do not intend to utilize SNMP, it is recommended that you delete both of the default community strings. If there are no community strings, then SNMP management access to the switch is disabled.

© 2004 Foundry Networks, Inc.

To prevent unauthorized access to the switch via SNMP, it is recommended that you change the default community strings.

To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server community *string mode*,” where “string” is the community access string and “mode” is **rw** (read/write) or **ro** (read only). Press <Enter>.
2. To remove an existing string, simply type “no snmp-server community *string*,” where “string” is the community access string to remove. Press <Enter>.

```
Console(config)#snmp-server community mis rw
Console(config)#snmp-server community private
Console(config)#
```

Trap Receivers

You can also specify SNMP stations that are to receive traps from the switch.

To configure a trap receiver, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server host *host-address community-string*,” where “host-address” is the IP address for the trap receiver and “community-string” is the string associated with that host. Press <Enter>.
2. In order to configure the switch to send SNMP notifications, you must enter at least one snmp-server enable traps command. Type “snmp-server enable traps *type*,” where “type” is either **authentication** or **link-up-down**. Press <Enter>.

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Saving Configuration Settings

Configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in non-volatile storage, you must copy the running configuration file to the start-up configuration file using the “copy” command.

To save the current configuration settings, enter the following command:

1. From the Privileged Exec mode prompt, type “copy running-config startup-config” and press <Enter>.
2. Enter the name of the start-up file. Press <Enter>.

© 2004 Foundry Networks, Inc.

```
Console#copy running-config startup-config
Startup configuration file name [startup]: startup
Write to FLASH Programming.
Write to FLASH finish.
Success.
Console#
```

Managing System Files

The switch's flash memory supports three types of system files that can be managed by the CLI program, Web interface, or SNMP. The switch's file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file.

The three types of files are:

- **Configuration** – These files store system configuration information and are created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via TFTP to a server for backup. A file named "Factory_Default_Config.cfg" contains all the system default settings and cannot be deleted from the system. See on page 3-13 for more information.
- **Operation Code** – System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI, Web and SNMP management interfaces. See on page 3-52 for more information.
- **Diagnostic Code** – Software that is run during system boot-up, also known as POST (Power On Self-Test). This code also provides a facility to upload firmware files to the system directly through the console port. See on page C-1.

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows.

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded.

 © 2004 Foundry Networks, Inc.

System Defaults

The switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg." To reset the switch defaults, this file should be set as the startup configuration file. See on page 3-13.

The following table lists some of the basic system defaults.

Function	Parameter	Default
IP Settings	Management VLAN	1
	DHCP	Enabled
	BOOTP	Disabled
	User Specified	Disabled
	IP Address	0.0.0.0
	Subnet Mask	255.0.0.0
	Default Gateway	0.0.0.0
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
SNMP	Community Strings	"public" (read only) "private" (read/write)
	Authentication Failure Traps	Enabled
	Link-up-Down Traps	Enabled
Security	Privileged Exec Level	Username "admin" Password "admin"
	Normal Exec Level	Username "guest" Password "guest"
	Enable Privileged Exec from Normal Exec Level	Password "super"
	Authentication	local
Console Port Connection	Baud Rate	9600
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)
Port Status	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
	10/100/1000 Mbps Port Capability	10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex 1000 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled
	Port Security	Learning is enabled

© 2004 Foundry Networks, Inc.

Function	Parameter	Default
Link Aggregation	Static Trunks	none
	LACP (all ports)	Disabled
Spanning Tree Protocol	Status	Disabled (Defaults: All parameters based on IEEE 802.1w)
	Fast Forwarding	Disabled
Address Table	Aging Time	300 seconds
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	GVRP (global)	Disabled
	GVRP (port interface)	Disabled
Class of Service	Ingress Port Priority	0
	Weighted Round Robin	EdgeIron 4802CF, 2402CF Class 0: 1 Class 1: 4 Class 2: 16 Class 3: 64 EdgeIron 24G Class 0: 16 Class 1: 64 Class 2: 128 Class 3: 240 EdgeIron 24G-A, 48G Class 0: 1 Class 1: 2 Class 2: 4 Class 3: 6 Class 4: 8 Class 5: 10 Class 6: 12 Class 7: 14
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
	IP Port Priority	Disabled
Multicast Filtering	IGMP Snooping	Enabled
	Act as Querier	Enabled
Broadcast Storm Protection	Status	Enabled (all ports)
	Broadcast Limit Rate	EdgeIron 4802CF, 2402CF 500 packets per second EdgeIron 24G-A, 24G, 48G 256 packets per second

 © 2004 Foundry Networks, Inc.

Function	Parameter	Default
System Log	Status	Enabled
	Messages Logged	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3

© 2004 Foundry Networks, Inc.

© 2004 Foundry Networks, Inc.

Chapter 3
Configuring the Switch

Using the Web Interface

This switch provides an embedded HTTP Web agent. Using a Web browser you can configure the switch and view statistics to monitor network activity. The Web agent can be accessed by any computer on the network using a standard Web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above).

Note: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to Chapter 4 “Command Line Interface.”

Prior to accessing the switch from a Web browser, be sure you have first performed the following tasks:

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See “Setting the IP Address” on page 3-10.)
2. Set user names and passwords using an out-of-band serial connection. Access to the Web agent is controlled by the same user names and passwords as the onboard configuration program. (See “Configuring the Logon Password” on page 3-24.)
3. After you enter a user name and password, you will have access to the system configuration program.

Notes: 1. You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

2. If you log into the Web interface as guest (Normal Exec level), you can view page information but only change the guest password. If you log in as “admin” (Privileged Exec level), you can apply changes on all pages.

3. If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Protocol, then you can set the switch port attached to your management station to fast forwarding to improve the switch’s response time to management commands issued through the Web interface. (See “STP Port and Trunk Configuration” on page 3-83.)

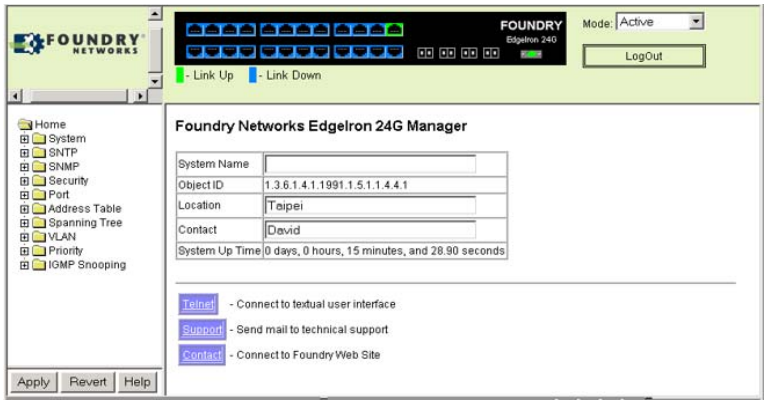
© 2004 Foundry Networks, Inc.

Navigating the Web Browser Interface

To access the Web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password for the administrator is “admin.”

Home Page

When your Web browser connects with the switch’s Web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics. (The following screen displays the EdgeIron 4802CF homepage.)



Configuration Options

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the “Apply” or “Apply Changes” button to confirm the new setting. The following table summarizes the Web page configuration buttons.

Button	Action
Revert	Cancels specified values and restores current values prior to pressing “Apply” or “Apply Changes.”
Refresh	Immediately updates values for the current page.
Apply	Sets specified values to the system.
Apply Changes	Sets specified values to the system.

Notes: 1. To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu “Tools / Internet Options / General / Temporary Internet Files / Settings,” the setting for item “Check for newer versions of stored pages” should be “Every visit to the page.”

2. When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser’s refresh button.

© 2004 Foundry Networks, Inc.

Panel Display

The Web agent displays an image of the switch's ports, indicating whether each link is up or down. Clicking on the image of a port opens the Port Configuration page as described on page 3-54.



Main Menu

Using the onboard Web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

Menu	Description	Page
System		
System Information	Provides basic system description, including contact information	3-6
Switch Information	Shows the number of ports, hardware/firmware version numbers, and power status	3-7
Bridge Extension	Shows the configuration for bridge extension command	3-52
IP	Sets the IP address for management access	3-10
File		
Firmware	Manages code image files	3-12
Configuration	Manages switch configuration files	3-13
Log		
Log	Stores and displays error messages	3-15
System Logs	Sends error messages to a logging process	3-16
Remote Logs	Configures the logging of messages to a remote logging process	3-17
SMTP	Sends an SMTP client message to a participating server	3-18
Reset	Restarts the switch	3-20
SNTP		
Configuration	Configures SNTP client settings, including broadcast mode or a specified list of servers	3-20
Clock Time Zone	Sets the local time zone for the system clock	3-22
SNMP		
SNMP Configuration	Configures community strings and related trap functions.	3-22
Security		
Passwords	Assigns a new password for the logon user name	3-24
Authentication Settings	Configures RADIUS and TACACS+ authentication parameters	3-25
HTTPS Settings	Configures secure HTTP settings.	3-27
SSH		
SSH Settings	Configures Secure Shell settings.	3-28
Host-Key Settings	Generates the host key pair (public and private)	3-30
Port Security Configuration	Configures port security on specified ports	3-32

© 2004 Foundry Networks, Inc.

Menu	Description	Page
802.1x		
Information	Displays general port authentication status information	3-36
Configuration	Enables the changing of general port authentication features	3-36
Port Configuration	Enables the changing of port authentication features	3-37
Port Statistics	Displays a per-port statistical readout	3-38
ACL		3-40
Configuration	Configures packet filtering based on IP or MAC addresses	3-40
Mask Configuration	Controls the order in which ACL rules are checked	3-46
Port Binding	Binds a port to the specified ACL	3-49
IP Filter	Sets IP addresses of clients allowed management access via the Web, SNMP, and Telnet	3-51
Port		
Port Information	Displays port connection status	3-52
Trunk Information	Displays trunk connection status	3-52
Port Configuration	Configures port connection settings	3-54
Trunk Configuration	Configures trunk connection settings	3-54
Trunk Members	Specifies ports to groups in static trunks	3-55
LACP		
Configuration	Allows ports to dynamically join trunks	3-57
Aggregation Port	Configures system priority, admin key, and port priority	3-60
Port Counters Information	Displays statistics for LACP protocol messages	3-61
Port Internal Information	Displays settings and operational state for local side	3-63
Port Neighbors Information	Displays settings and operational state for remote side	3-63
Broadcast Storm Protect Configuration	Sets the broadcast control threshold for each port	3-64
Mirror Port Configuration	Sets the source and target ports for mirroring	3-66
Rate Limit		
Rate Limit Configuration	Sets the rate limit for each port	3-67
Address Table		
Static Addresses	Displays entries for interface, address or VLAN	3-69
Dynamic Addresses	Displays or edits static entries in the Address Table	3-70
Address Aging	Sets timeout for dynamically learned entries	3-71
Spanning Tree		
STP Information	Displays STP values used for the bridge	3-74
STP Configuration	Configures global bridge settings for STP	3-77
STP Port Information	Configures individual port settings for STP	3-81
STP Trunk Information	Configures individual trunk settings for STP	3-81
STP Port Configuration	Configures individual port settings for STP	3-83
STP Trunk Configuration	Configures individual trunk settings for STP	3-83

 © 2004 Foundry Networks, Inc.

Menu	Description	Page
Multiple Spanning Tree		
VLAN Configuration	Configures priority and VLANs for a spanning tree instance	3-85
Port Information	Displays port settings for a specified MST instance	3-87
Trunk Information	Displays trunk settings for a specified MST instance	3-87
Port Configuration	Configures port settings for a specified MST instance	3-89
Trunk Configuration	Configures trunk settings for a specified MST instance	3-89
VLAN		
VLAN Basic Information	Displays basic information on the VLAN type supported by this switch	3-92
VLAN Current Table	Shows the current port members of each VLAN and whether or not the port supports VLAN tagging	3-93
VLAN Static List	Used to create or remove VLAN groups	3-95
VLAN Static Table	Modifies the settings for an existing VLAN	3-96
VLAN Static Membership by Port	Configures membership type for interfaces, including tagged or untagged	3-98
VLAN Port Configuration	Specifies default PVID and VLAN attributes	3-98
VLAN Trunk Configuration	Specifies default trunk VID and VLAN attributes	3-98
Private VLAN		
Status	Enables or disables the private VLAN	3-101
Link Status	Configures the private VLAN	3-101
Priority		
Default Port Priority	Sets the default priority for each port	3-102
Default Trunk Priority	Sets the default priority for each trunk	3-102
Traffic Class	Maps IEEE 802.1p priority tags to output queues	3-103
Queue Scheduling	Configures Weighted Round Robin queueing	3-105
IP Precedence/DSCP Priority Status	Globally selects IP Precedence or DSCP Priority, or disables both	3-106
IP Precedence Priority	Sets IP Type of Service priority, mapping the precedence tag to a class-of-service value	3-107
IP DSCP Priority	Sets IP Differentiated Services Code Point priority, mapping a DSCP tag to a class-of-service value	3-109
IP Port Priority Status	Globally enables or disables IP Port Priority	3-110
IP Port Priority	Sets TCP port priority, defining the socket number and associated class-of-service value	3-110
ACL CoS Priority	Sets the CoS value and corresponding output queue for packets matching an ACL rule	3-112
ACL Marker	Change traffic priorities for frames matching an ACL rule	3-113
Statistics	Lists Ethernet and RMON port statistics	3-120
IGMP		
IGMP Configuration	Enables multicast filtering; configures parameters for multicast query	3-115
Multicast Router Port Information	Displays the ports that are attached to a neighboring multicast router/switch for each VLAN ID	3-116

© 2004 Foundry Networks, Inc.

Menu	Description	Page
Static Multicast Router Port Configuration	Assigns ports that are attached to a neighboring multicast router/switch	3-117
IP Multicast Registration Table	Displays all multicast groups active on this switch, including multicast IP addresses and VLAN ID	3-119
IGMP Member Port Table	Indicates multicast addresses associated with the selected VLAN	3-118

Basic Configuration

Displaying System Information

You can easily identify the system by providing a descriptive name, location and contact information.

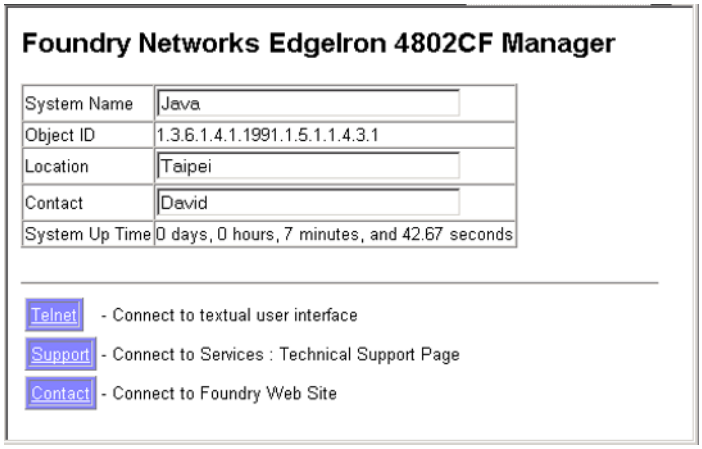
Command Attributes

- **System Name** – Name assigned to the switch system.
- **Object ID** – MIB II object ID for switch's network management subsystem.
- **Location** – Specifies the system location.
- **Contact** – Administrator responsible for the system.
- **System Up Time** – Length of time the management agent has been up.
- **MAC Address*** – The physical layer address for the switch.
- **Web server*** – Shows if management access via HTTP is enabled or disabled.
- **Web server port*** – Shows the TCP port number used by the Web interface.
- **Web secure server*** – Shows if management access via secure HTTP (HTTPS) is enabled or disabled.
- **Web secure server port*** – Shows the TCP port number used by the HTTPS server.
- **POST result*** – Shows results of the power-on self-test

* CLI Only

© 2004 Foundry Networks, Inc.

Web – Click System, System Information. Specify the system name, location, and contact information for the system administrator, then click Apply. (This page also includes a Telnet button that allows you to access the Command Line Interface via Telnet.)



CLI – Specify the hostname, location and contact information.

```
Console(config)#hostname Java                                    4-20
Console(config)#snmp-server location Taipei                      4-92
Console(config)#snmp-server contact David                        4-92
Console#show system                                              4-46
System description: Foundry Networks EdgeIron 24G
System OID string: 1.3.6.1.4.1.1991.1.5.1.1.4.4.1
System information
 System Up time: 0 days, 0 hours, 22 minutes, and 43.97 seconds
 System Name            : Java
 System Location        : Taipei
 System Contact         : David
 MAC address            : 00-04-80-BD-47-4D
 Web server             : enable
 Web server port        : 80
 Web secure server      : enable
 Web secure server port : 443
 POST result
UART LOOP BACK Test.........PASS
DRAM Test...................PASS
Timer Test..................PASS
PCI Device 1 Test...........PASS
PCI Device 2 Test...........PASS
Switch Int Loopback test.....PASS

Done All Pass.
Console#
```

Displaying Switch Hardware/Software Versions

Use the Switch Information page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

Command Attributes

Main Board

- **Serial Number** – The serial number of the switch.
- **Number of Ports** – Number of built-in RJ-45 ports
- **Hardware Version** – Hardware version of the main board.

© 2004 Foundry Networks, Inc.

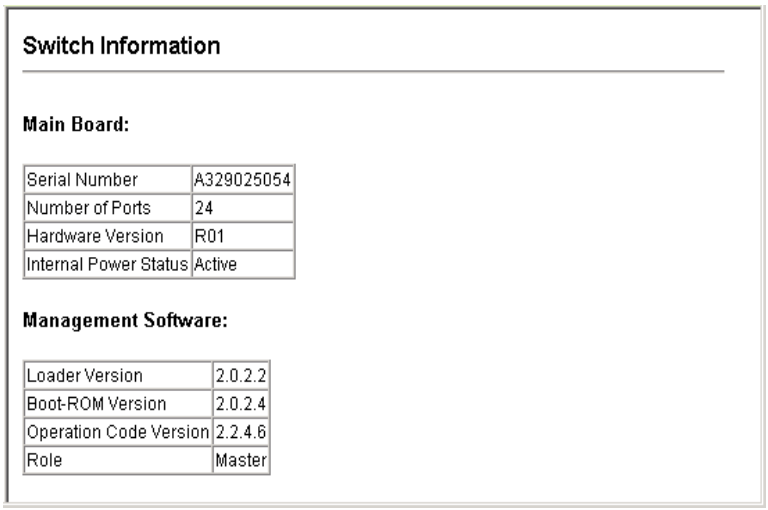
- **Internal Power Status** – Displays the status of the internal power supply.
- **Redundant Power Status*** – Displays the status of the redundant power supply.

* CLI only.

Management Software

- **Loader Version** – Version number of loader code.
- **Boot-ROM Version** – Version number of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.
- **Role** – Shows that this switch is operating as Master (i.e., operating stand-alone).

Web – Click System, Switch Information.



Switch Information

Main Board:

Serial Number	A329025054
Number of Ports	24
Hardware Version	R01
Internal Power Status	Active

Management Software:

Loader Version	2.0.2.2
Boot-ROM Version	2.0.2.4
Operation Code Version	2.2.4.6
Role	Master

CLI – Use the following command to display version information.

```
Console#show version                                          4-48
Unit1
 Serial number          :A329025054
 Hardware version       :R01
 Number of ports        :24
 Main power status      :up
 Redundant power status :not present
Agent(master)
 Unit id                :1
 Loader version         :2.0.2.2
 Boot rom version       :2.0.2.4
 Operation code version :2.2.4.11
Console#
```

Displaying Bridge Extension Capabilities

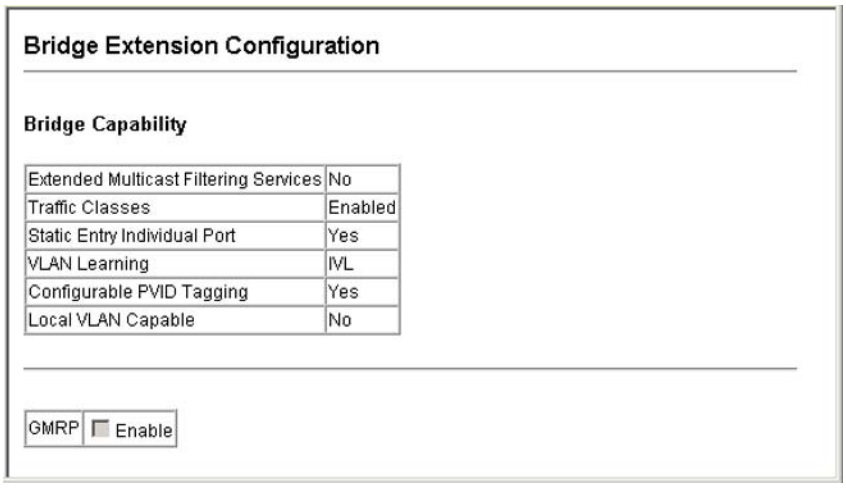
The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables, or to configure the global setting for GARP VLAN Registration Protocol (GVRP).

 © 2004 Foundry Networks, Inc.

Command Attributes

- **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to “Priority Configuration” on page 3-102.)
- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to “Setting Static Addresses” on page 3-69.)
- **VLAN Learning** – This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
- **Configurable PVID Tagging** – This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to “VLAN Configuration” on page 3-90.)
- **Local VLAN Capable** – This switch supports multiple local bridges (i.e., multiple Spanning Trees).
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

Web – Click System, Bridge Extension.



CLI – Enter the following command.

```
Console#show bridge-ext                                          4-157
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Enabled
 GMRP: Disabled
Console#
```

 © 2004 Foundry Networks, Inc.

Setting the IP Address

An IP address may be used for management access to the switch over your network. By default, the switch uses DHCP to assign IP settings to VLAN 1 on the switch. If you wish to manually configure IP settings, you need to change the switch's user-specified defaults (IP address 0.0.0.0 and netmask 255.0.0.0) to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment.

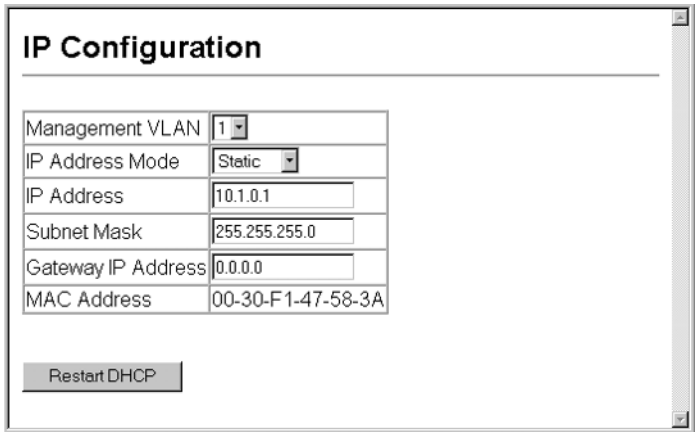
You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server when it is powered on. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

- **Management VLAN** – This is the only VLAN through which you can gain management access to the switch. By default, all ports on the switch are members of VLAN 1, so a management station can be connected to any port on the switch. However, if other VLANs are configured and you change the Management VLAN, you may lose management access to the switch. In this case, you should reconnect the management station to a port that is a member of the Management VLAN.
- **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. (DHCP/BOOTP values can include the IP address, subnet mask, and default gateway.)
- **IP Address** – Address of the VLAN interface that is allowed management access. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets.
- **Gateway IP Address** – IP address of the gateway router between this device and management stations that exist on other network segments.
- **MAC Address** – The MAC address of this switch.

 © 2004 Foundry Networks, Inc.

Manual Configuration

Web – Click System, IP. Specify the management interface, IP address and default gateway, then click Apply.



CLI – Specify the management interface, IP address and default gateway.

```
Console#config                                              4-10
Console(config)#interface vlan 1                           4-109
Console(config-if)#ip address 10.2.13.30 255.255.255.0      4-97
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254            4-98
Console(config)#
```

Using DHCP/BOOTP

If your network provides DHCP/BOOTP services, you can configure the switch to be dynamically configured by these services.

Web – Click System, IP. Specify the Management VLAN, set the IP Address Mode to DHCP or BOOTP. Then click Apply to save your changes. The switch will broadcast a request for IP configuration settings on the next power reset. Otherwise, you can click Restart DHCP to immediately request a new address.

If you lose your management connection, use a console connection and enter **show ip interface** to determine the new switch address.

CLI – Specify the management interface, and set the IP Address Mode to DHCP or BOOTP.

```
Console(config)#interface vlan 1                           4-109
Console(config-if)#ip address dhcp                          4-97
Console(config-if)#end
Console#ip dhcp restart                                     4-98
Console#show ip interface                                   4-99
IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#
```

Renewing DCHP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. In this case, you can reboot the switch or submit a client request to restart DHCP service.

© 2004 Foundry Networks, Inc.

Web – If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the Web interface. You can only restart DHCP service via the Web interface if the current address is still available.

CLI – Enter the following command to restart DHCP service.

```
Console#ip dhcp restart                                    4-98
```

Managing Firmware

You can upload/download firmware to or from a TFTP server. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the switch to restore operation. You can also set the switch to use new firmware without overwriting the previous version.

Command Attributes

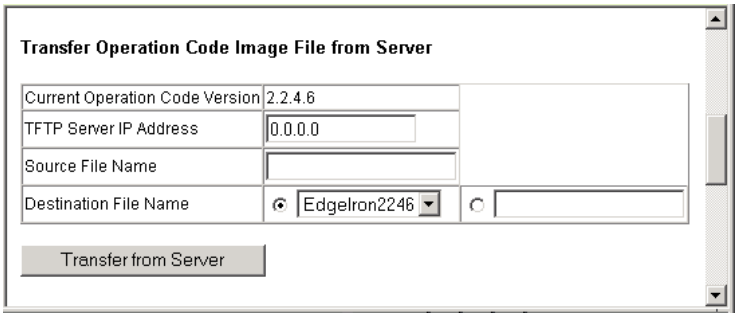
- **TFTP Server IP Address** – The IP address of a TFTP server.
- **Destination File Name** – File names are case-sensitive, should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

Note: The maximum number of runtime code files is two.

Downloading System Software from a Server

When downloading runtime code, you can specify the Destination File Name to replace the current image, or first download the file using a different name from the current runtime code file, and then set the new file as the startup file.

Web – Click System, Firmware. Enter the IP address of the TFTP server, enter the file name of the software to download, select a file on the switch to overwrite or specify a new file name, then click Transfer from Server.



 © 2004 Foundry Networks, Inc.

When you download a file using a different name from the current runtime code file, you need to select the new file name from the drop-down box for the operation code used at startup, and then click Apply Changes.



To start the new firmware, reboot the system.

CLI – Enter the IP address of the TFTP server, select **config** or **opcode** file type, then enter the source and destination file names, set the new file to start up the system, and then restart the switch.

```
Console#copy tftp file                                          4-14
TFTP server ip address: 10.1.0.99
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: v10.bix
Destination file name: V10000
/
Console#config
Console(config)#boot system opcode: V10000                      4-17
Console(config)#exit
Console#reload                                                  4-11
```

Saving or Restoring Configuration Settings

You can upload/download configuration settings to/from a TFTP server. The configuration file can be later downloaded to restore the switch's settings.

Command Attributes

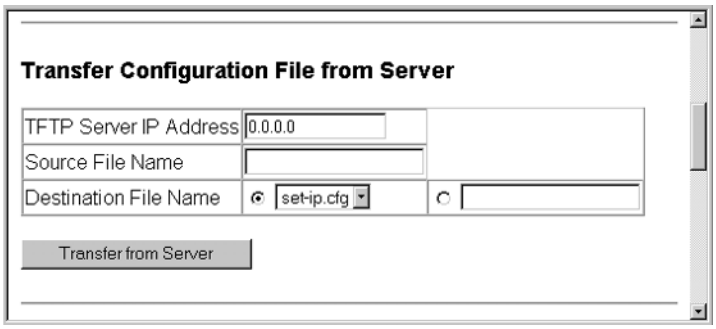
- **TFTP Server IP Address** – The IP address of a TFTP server.
- **Destination File Name** – File names are case-sensitive, should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

Note: The maximum number of user-defined configuration files is limited only by available flash memory space.

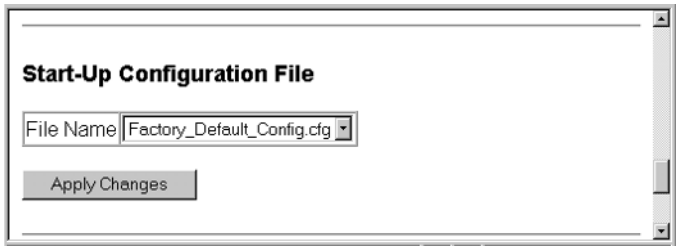
You can save the configuration file under a new file name and then set it as the startup file, or you can specify the current startup configuration file as the destination file to directly replace it. Note that the file "Factory_Default_Config.cfg" can be copied to the TFTP server, but cannot be used as a destination file name on the switch.

 © 2004 Foundry Networks, Inc.

Web – Click System, Configuration. Enter the IP address of the TFTP server, enter the name of the file to download, select a file on the switch to overwrite or specify a new file name, and then click Transfer from Server.



If you download to a new file name, select the new file from the drop-down box for Startup Configuration File, and click Apply Changes. To use the new settings, reboot the system via the System/Reset menu.



CLI – Enter the IP address of the TFTP server, specify the source file on the server, and set the startup file name on the switch. If you download the startup configuration file under a new file name, you can set this file as the startup file at a later time, and then restart the switch.

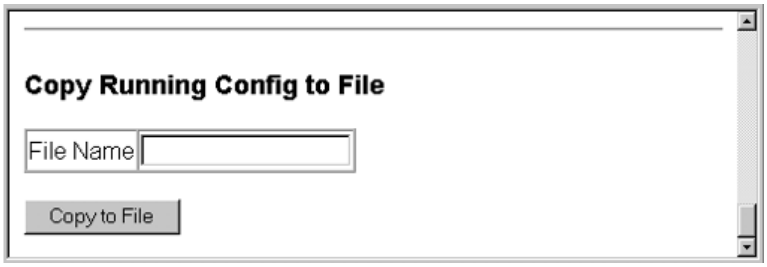
```
Console#copy tftp startup-config                                    4-14
TFTP server ip address: 192.168.1.19
Source configuration file name: startup2.0
Startup configuration file name [startup] : startup2.0
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#config
Console(config)#boot system config: startup2.0                      4-17
Console(config)#exit
Console#reload
```

 © 2004 Foundry Networks, Inc.

Copying the Running Configuration to a File

You can save the current running configuration to a new file name and then set it as the startup file. Enter a name for the new configuration file, and then click Copy to File.



CLI – If you copy the running configuration to a file, you can set this file as the startup file at a later time, and then restart the switch.

```
Console#copy running-config file                                    4-14
destination file name : 051902.cfg
/
Console#
Console#config
Console(config)#boot system config: 051902.cfg                      4-17
Console(config)#exit
Console#reload                                                      4-11
```

System Logs

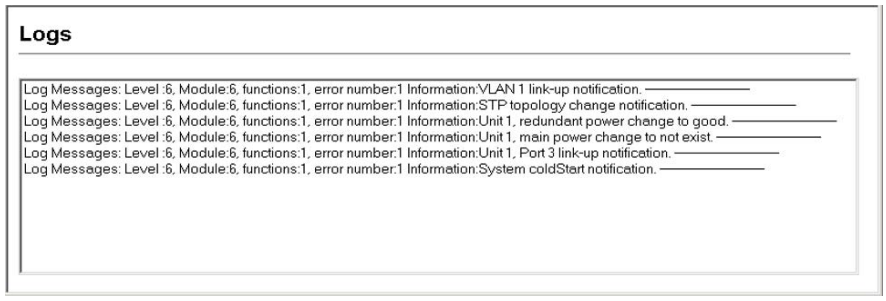
The system can be configured to send debug and error messages to a logging process. This logging process controls the type of error messages that are stored in switch memory or sent to a remote syslog server.

The system allows you to specify which levels are logged to RAM or flash memory.

Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded.

The Logs page allows you to scroll through the logged system and event messages. The switch can store up to 2048 log entries in temporary random access memory (RAM; i.e., memory flushed on power reset) and up to 4096 entries in permanent flash memory.

Web – Click System, Logs.


Logs
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:VLAN 1 link-up notification.
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:STP topology change notification.
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:Unit 1, redundant power change to good.
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:Unit 1, main power change to not exist.
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:Unit 1, Port 3 link-up notification.
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:System coldStart notification.

 © 2004 Foundry Networks, Inc.

CLI – Type "show logging" followed by the type of logging information required.

```
Console#sh logging sendmail                                    4-42
SMTP servers
-------------------------------------------

Active SMTP server: 0.0.0.0

SMTP minimum severity level: 7

SMTP destination email addresses
-------------------------------------------

SMTP source email address:

SMTP status: Enable
Console#
```

System Logs Configuration

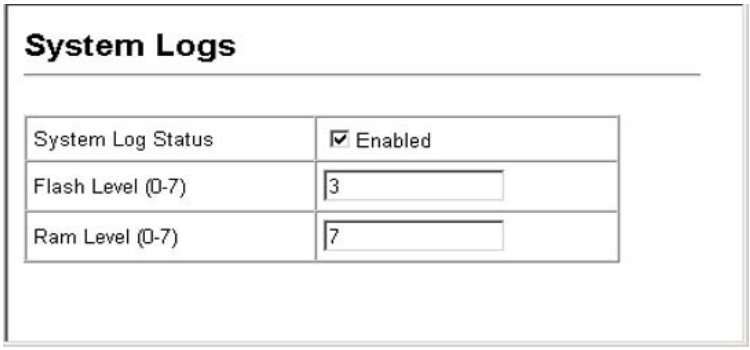
The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

Command Attributes

- **System Log Status** – Enables/disables the logging of debug or error messages to the logging process.
- **Flash Level** – Limits log messages saved to the switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash.
- **RAM Level** – Limits log messages saved to the switch's temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM.

Note: The Flash Level must be equal to or less than the RAM Level.

Web – Click System, System Logs. Specify System Log Status, then change the level of messages, and click Apply.



 © 2004 Foundry Networks, Inc.

CLI – Specify the hostname, location and contact information.

```
Console(config)#logging on                                    4-37
Console(config)#logging history ram 0                         4-38
Console(config)#
Console#show logging flash                                    4-42
Syslog logging: Enable
History logging in FLASH: level errors
[9] 13:30:42 2/28/4
   "VLAN 1 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[8] 13:30:42 2/28/4
   "STP topology change notification."
   level: 6, module: 6, function: 1, and event no.: 1
[7] 13:30:12 2/28/4
   "Unit 1, Port  8 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[6] 13:30:8 2/28/4
   "Unit 1, Port  8 link-down notification."
   level: 6, module: 6, function: 1, and event no.: 1
[5] 13:30:8 2/28/4
   "VLAN 1 link-down notification."
   level: 6, module: 6, function: 1, and event no.: 1
[4] 13:20:6 3/3/4
   "VLAN 1 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[3] 13:20:6 3/3/4
   "STP topology change notification."
   level: 6, module: 6, function: 1, and event no.: 1
[2] 13:19:36 3/3/4
   "Unit 1, Port  8 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[1] 13:19:31 3/3/4
   "Unit 1, Port  6 link-down notification."
   level: 6, module: 6, function: 1, and event no.: 1
[0] 13:19:31 3/3/4
   "VLAN 1 link-down notification."
   level: 6, module: 6, function: 1, and event no.: 1
Console#
```

Remote Logs Configuration

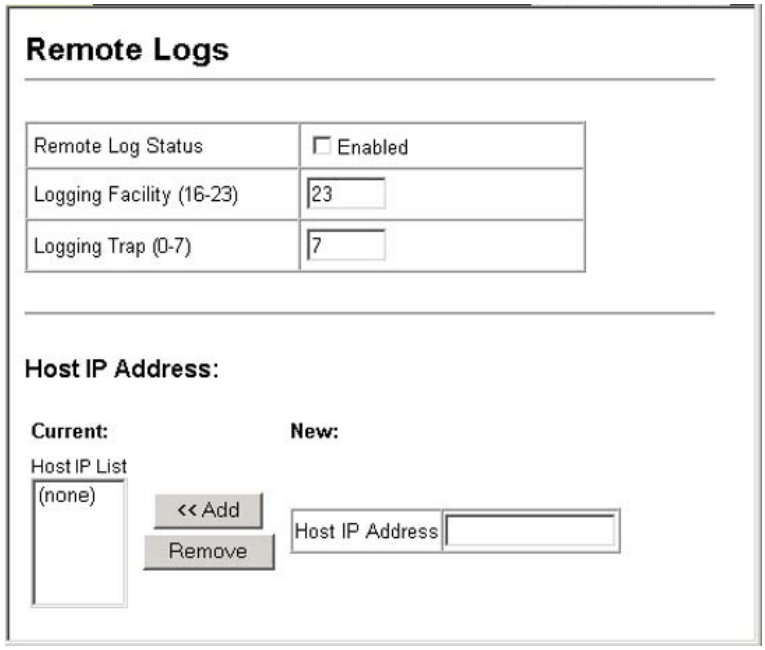
The Remote Logs page allows you to configure the logging of messages that are sent to syslog servers or other management stations. You can also limit the error messages sent to only those messages of a specified level.

Command Attributes

- **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process. (Default: enabled)
- **Logging Facility** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service. (Default: 23)
- **Logging Trap** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Default: 7)
- **Host IP List** – Displays the list of remote server IP addresses that receive the syslog messages. The maximum number of host IP addresses allowed is five.
- **Host IP Address** – Specifies a new server IP address to add to the Host IP List.

 © 2004 Foundry Networks, Inc.

Web – Click System, Remote Logs. To add an IP address to the Host IP List, type the new IP address in the Host IP Address box, and then click Add IP. To delete an IP address, click the entry in the Host IP List, and then click Remove.



CLI – Enter the syslog server host IP address, choose the facility type and set the logging trap.

```
Console(config)#logging host 10.1.0.9                          4-39
Console(config)#logging facility 23                            4-39
Console(config)#logging trap 4                                 4-40
Console(config)#end
Console#show logging trap                                      4-42
Syslog logging: Enable
REMOTELOG status: enable
REMOTELOG facility type: local use 7
REMOTELOG level type: Warning conditions
REMOTELOG server ip address: 10.1.0.9
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
Console#
```

Sending Simple Mail Transfer Protocol Alerts

To alert system administrators of problems, the switch can use SMTP (Simple Mail Transfer Protocol) to send email messages when triggered by logging events of a specified level. The messages are sent to specified SMTP servers on the network and can be retrieved using POP or IMAP clients.

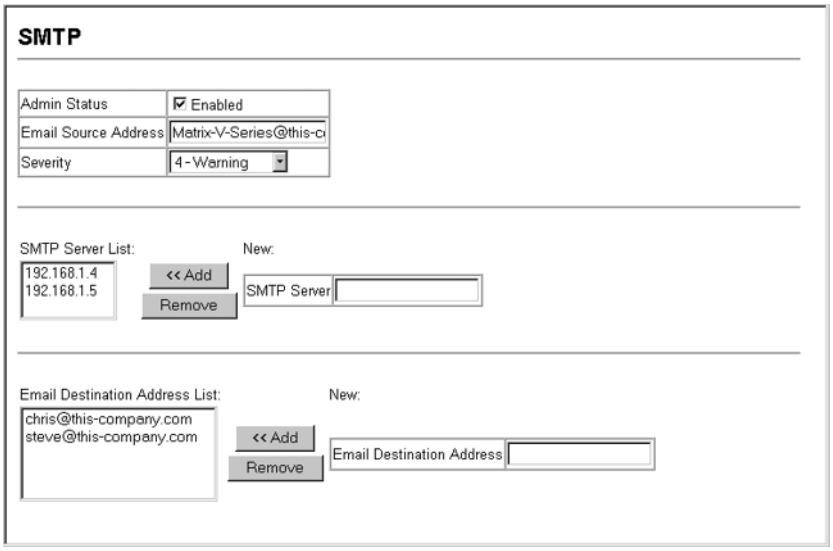
Command Attributes

- **Admin Status** – Enables/disables the SMTP function. (Default: Disabled)
- **Email Source Address** – Sets the email address used for the “From” field in alert messages. You may use a symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

 © 2004 Foundry Networks, Inc.

- **Severity** – Sets the syslog severity threshold level (see table “Syslog Definition” on page 4-38) used to trigger alert messages. All events at this level or higher will be sent to the configured email recipients. For example, using Level 7 will report all events from level 7 to level 0. (Default : Level 7)
- **SMTP Server List** – Specifies a list of up to three recipient SMTP servers. The switch attempts to connect to the other listed servers if the first fails. Use the New SMTP Server text field and the Add/Remove buttons to configure the list.
- **Email Destination Address List** – Specifies the email recipients of alert messages. You can specify up to five recipients. Use the New Email Destination Address text field and the Add/Remove buttons to configure the list.

Web – Click System, Log, SMTP. Enable SMTP, specify a source email address, and select the minimum severity level. To add an IP address to the SMTP Server List, type the new IP address in the SMTP Server text box and then click Add. To delete an IP address, click the entry in the SMTP Server List and then click Remove. Specify up to five email addresses to receive the alert messages, and then click Apply.



 © 2004 Foundry Networks, Inc.

CLI – Enter the IP address of at least one SMTP server, set the syslog severity level to trigger an email message, and specify the switch (source) and up to five recipient (destination) email addresses. Enable SMTP with the **logging sendmail** command to complete the configuration. Use the **show logging sendmail** command to display the current SMTP configuration.

```
Console(config)#logging sendmail host 192.168.1.4              4-48
Console(config)#logging sendmail level 3                       4-49
Console(config)#logging sendmail source-email
   fred@this-company.com                                       4-50
Console(config)#logging sendmail destination-email
   chris@this-company.com                                      4-50
Console(config)#logging sendmail                               4-50
Console(config)#exit
Console#show logging sendmail                                  4-51
SMTP servers
-----------------------------------------------
  1. 192.168.1.4

Active SMTP server: 0.0.0.0

SMTP minimum severity level: 4

SMTP destination email addresses
-----------------------------------------------
  1. chris@this-company.com

SMTP source email address:   Foundry@this-company.com

SMTP status:               Enabled
Console#
```

Resetting the System

Web – Select System, Reset to reboot the switch. When prompted, confirm that you want reset the switch.



CLI – Use the **reload** command to reboot the system.

```
Console#reload                                                 4-11
System will be restarted, continue <y/n>? y
Console#
```

Note: When restarting the system, it always runs the Power-On Self-Test.

Configuring SNTP

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock using the CLI. (See “calendar set” on page 4-55.) If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

 © 2004 Foundry Networks, Inc.

This switch acts as an SNTP client in two modes:

Unicast – The switch periodically sends a request for a time update to a configured time server. You can configure up to three time server IP addresses. The switch will attempt to poll each server in the configured sequence.

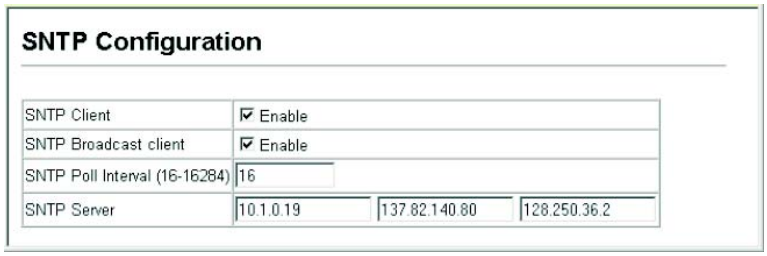
Broadcast – The switch sets its clock from a time server in the same subnet that broadcasts time updates. If there is more than one SNTP server, the switch accepts the first broadcast it detects and ignores broadcasts from other servers.

You can configure the switch to send time synchronization requests to specific time servers (i.e., client mode), update its clock based on broadcasts from time servers, or use both methods. When both methods are enabled, the switch will update its clock using information broadcast from time servers, but will query the specified server(s) if a broadcast is not received within the polling interval.

Command Attributes

- **SNTP Client** – Configures the switch to operate as an SNTP unicast client. This mode requires at least one time server to be specified in the SNTP Server field.
- **SNTP Broadcast Client** – Configures the switch to operate as an SNTP broadcast client. This mode requires no other configuration settings; the switch will obtain time updates from time server broadcasts (using the multicast address 224.0.1.1).
- **SNTP Poll Interval** – Sets the interval between sending requests for a time update from a time server when set to SNTP Client mode. (Range: 16-16284 seconds; Default: 16 seconds)
- **SNTP Server** – In unicast mode, sets the IP address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

Web – Select SNTP, Configuration. Modify any of the required parameters, and click Apply.



CLI – This example configures the switch to operate as an SNTP broadcast client.

```
Console(config)#sntp client                                    4-52
Console(config)#sntp poll 16                                   4-53
Console(config)#sntp server 10.1.0.19 137.82.140.80
   128.250.36.2                                                4-52
Console(config)#sntp broadcast client
Console(config)#
```


© 2004 Foundry Networks, Inc.

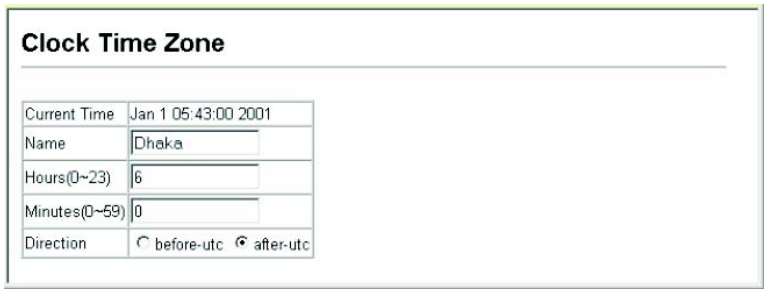
Setting the Time Zone

SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Command Attributes

- **Current Time** – Displays the current time.
- **Name** – Assigns a name to the time zone.
- **Hours (0-12)** – The number of hours before/after UTC**.**
- **Minutes (0-59)** – The number of minutes before/after UTC.
- **Direction** – Configures the time zone to be before (east) or after (west) UTC.

Web – Select SNTP, Clock Time Zone. Set the offset for your time zone relative to the UTC, and click Apply.



CLI - This example shows how to set the time zone for the system clock.

```
Console(config)#clock timezone Dhaka hours 6 minute 0 after-UTC
Console#
```

Configuring SNMP

The switch includes an onboard agent that continuously monitors the status of its hardware, as well as the traffic passing through its ports, based on the Simple Network Management Protocol (SNMP). A network management station can access this information using management software. Access rights to the onboard agent are controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following sections.

Setting Community Access Strings

You may configure up to five community strings authorized for management access. For security reasons, you should consider removing the default strings.

Command Attributes

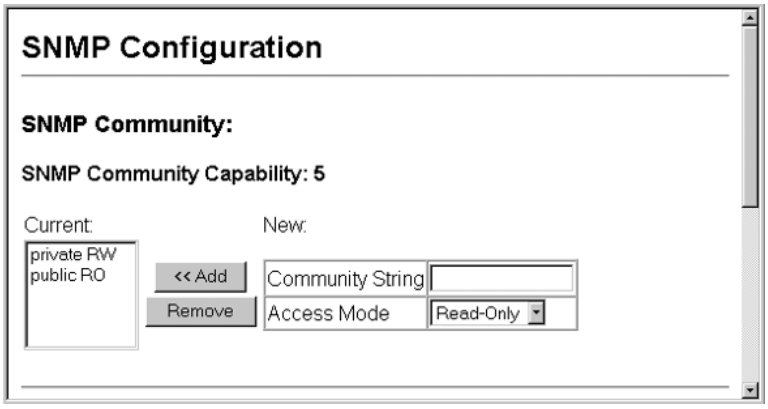
Community String – A community string that acts like a password and permits access to the SNMP protocol.

 © 2004 Foundry Networks, Inc.

Access Mode

- **Read-Only** – Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **Read/Write** – Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Web – Click SNMP, SNMP Configuration. Enter a new string in the Community String box and select the access rights from the Access Mode drop-down list, then click Add.



CLI – The following example adds the string “spiderman” with read/write access.

```
Console(config)#snmp-server community spiderman rw            4-91
Console(config)#
```

Specifying Trap Managers

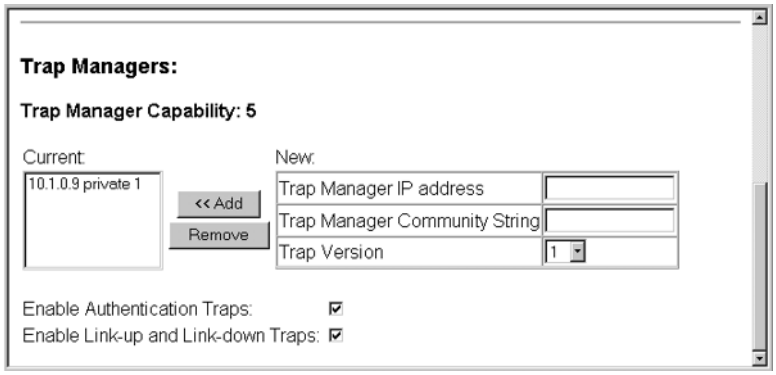
You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

Command Usage

- If you do not enter a trap manager host IP address, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one host IP address.
- The switch can send SNMP version 1 or version 2c traps to a host IP address, depending on the SNMP version that the management station supports. The default is to send SNMP version 1 traps.
- You can enable or disable authentication messages and link-up-down messages via the Web interface.
- You can enable or disable authentication messages, link-up-down messages, or all notification types via the CLI.

© 2004 Foundry Networks, Inc.

Web – Click SNMP, SNMP Configuration. Fill in the Trap Manager IP Address box and the Trap Manager Community String box, mark Enable Authentication Traps if required, and then click Add.



CLI – This example adds a trap manager and enables authentication traps.

```
Console(config)#snmp-server host 10.1.19.23 batman            4-93
Console(config)#snmp-server enable traps authentication       4-94
```

Security

Configuring the Logon Password

The guest only has read access for most configuration parameters. However, the administrator has write access for parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place. (If for some reason your password is lost, you can reload the factory deafults file to restore the default passwords as described in “Troubleshooting Chart” on page B-1.)

The default guest name is “guest” with the password “guest.” The default administrator name is “admin” with the password “admin.” Note that user names can only be assigned via the CLI.

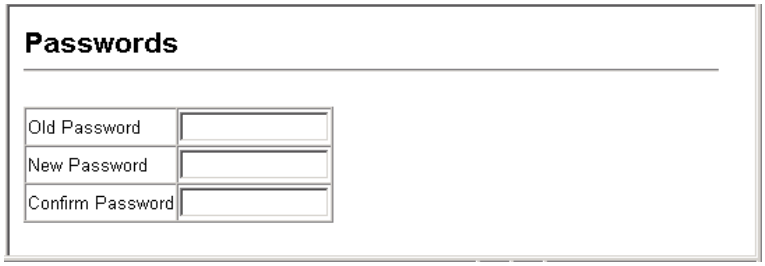
Command Attributes

- **User Name*** – The name of the user.
  (Maximum length: 8 characters, case sensitive; maximum number of users: 16)
- **Access Level*** – Specifies the user level.
  (Options: 0 - Normal, 15 - Privileged.)
- **Password** – Specifies the user password.
  (Range: 0-8 characters plain text, case sensitive)

* CLI only.

© 2004 Foundry Networks, Inc.

Web – Click System, Passwords. To change the password for the current user, enter the old password, then enter the new password, confirm it by entering it again, then click Apply.



CLI – Assign a user name to access-level 15 (i.e., administrator), then specify the password.

```
Console(config)#username bob access-level 15                    4-20
Console(config)#username bob password 0 smith
Console(config)#
```

Configuring RADIUS/TACACS Logon Authentication

You can configure this switch to authenticate users logging into the system for management access using local, RADIUS, or TACACS+ authentication methods.

RADIUS and TACACS+ are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS+-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to a switch.

Like RADIUS, Terminal Access Controller Access Control System Plus (TACACS+) is a system that uses a central server to control authentication for access to switches on the network.

RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

Command Usage

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence and the corresponding parameters for the remote authentication protocol.
- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication control management access via the console port, Web browser, or Telnet. These access options must be configured on the authentication server.
- RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server.

 © 2004 Foundry Networks, Inc.

- You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

Command Attributes

- **Authentication** – Select the authentication, or authentication sequence required:
  - **RADIUS** – User authentication is performed using a RADIUS server only.
  - **TACACS** – User authentication is performed using a TACACS+ server only.
  - **Local** – User authentication is performed only locally by the switch.
  - **[authentication sequence]** – User authentication is performed by up to three authentication methods in the indicated sequence.

RADIUS Settings

- **Server IP Address** – Address of the RADIUS server.
  (Default: 10.1.0.1)
- **Server Port Number** – Network (UDP) port of the RADIUS server used for authentication messages.
  (Range: 1-65535; Default: 1812)
- **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string.
  (Maximum length: 20 characters)
- **Number of Server Transmits** – Number of times the switch will try to authenticate logon access via the RADIUS server.
  (Range: 1-30; Default: 2)
- **Timeout for a reply (secs)** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)

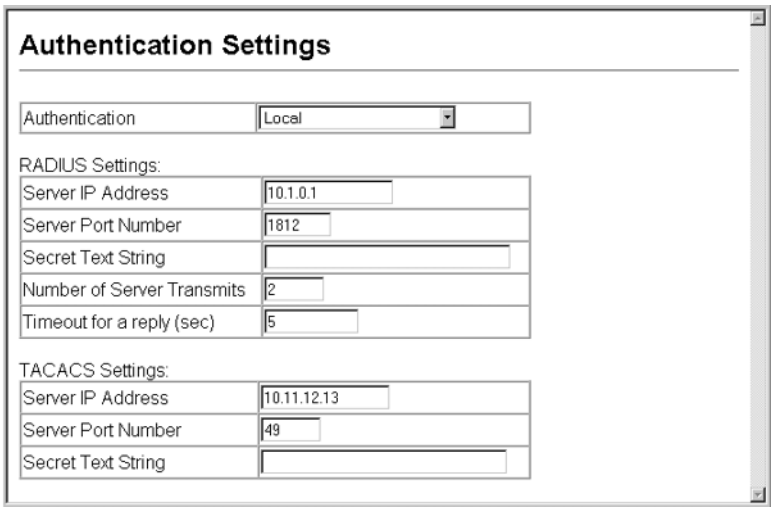
TACACS+ Settings

- **Server IP Address** – Address of the TACACS+ server.
  (Default: 10.1.0.1)
- **Server Port Number** – Network (TCP) port of TACACS+ server used for authentication messages.
  (Range: 1-65535; Default: 1812)
- **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string.
  (Maximum length: 20 characters)

Note: The local switch user database has to be set up by manually entering user names and passwords using the CLI.

 © 2004 Foundry Networks, Inc.

Web – Click System, Authentication Settings. To configure local or remote authentication preferences, specify the authentication sequence (i.e., one to three methods), fill in the parameters for RADIUS or TACACS+ authentication if selected, and click Apply.



CLI Commands

CLI – Specify all the required parameters to enable logon authentication.

```
Console(config)#authentication login radius                    4-57
Console(config)#radius-server host 192.168.1.25                4-58
Console(config)#radius-server port 181                         4-59
Console(config)#radius-server key green                        4-59
Console(config)#radius-server retransmit 5                     4-60
Console(config)#radius-server timeout 10                       4-60
Console#show radius-server                                     4-60
Server IP address: 192.168.1.25
 Communication key with radius server: green
 Server port number: 181
 Retransmit times: 5
 Request timeout: 10
Console(config)#authentication login tacacs                    4-57
Console(config)#tacacs-server host 10.20.30.40                 4-61
Console(config)#tacacs-server port 200                         4-61
Console(config)#tacacs-server key green                        4-62
Console#show tacacs-server                                     4-62
Server IP address: 10.20.30.40
 Communication key with tacacs server: green
 Server port number: 200
Console(config)#
```

HTTPS

You can configure the switch to enable the Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's Web interface.

Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port. If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: https://device:port_number.

 © 2004 Foundry Networks, Inc.

Note: If you enable HTTPS, you must indicate this in the URL.
For example: https://device [:port_number]

The following Web browsers and operating systems currently support HTTPS:

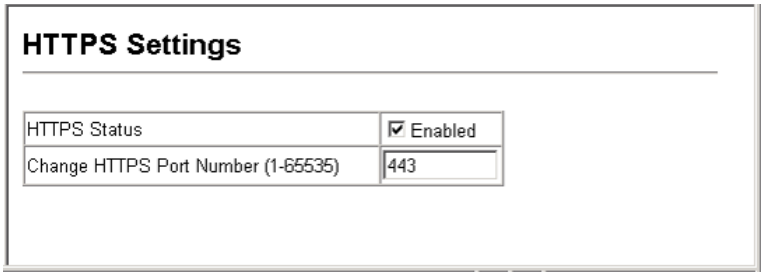
Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98, Windows NT (with service pack 6a), Windows 2000
Netscape Navigator 4.76 or later	Windows 98, Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

When you start HTTPS, the client and server establish a secure encrypted connection. A padlock icon should appear in the status bar for Internet Explorer 5.x and Netscape Navigator 4.x.

Command Attributes

- **HTTPS Status** – Allows you to enable/disable the HTTPS server on the switch. (Default: Enabled)
- **HTTPS Port** – Specifies the UDP port number used for HTTPS/SSL connection to the switch's Web interface. The default is port 443.

Web – Click System, HTTPS Settings. Select Enabled for the HTTPS Status and specify the port number, then click Apply.



CLI – Enter the following commands to specify the secure port number and to enable HTTPS.

```
Console(config)#ip http secure-server                          4-25
Console(config)#ip http secure-port 441                        4-26
Console(config)#
```

SSH

The Berkeley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rlogin* (remote login), *rsh* (remote shell), and *rcp* (remote copy), are not secure from hostile attacks. The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When the client contacts the switch via the SSH protocol, the switch generates a public-key that the client uses along with a local user name and password for access authentication. SSH also encrypts all data transfers

 © 2004 Foundry Networks, Inc.

passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered. Note that you need to install an SSH client on the management station to access the switch for management via the SSH protocol.

Note: The switch supports both SSH Version 1.5 and 2.0.There are two versions of the SSH protocol currently available, SSH v1.5 and SSH v2.0. The switch supports SSH v2.0.

To use the SSH server, complete these steps:

1. *Generate a Host Key Pair* – On the SSH Host Key Settings page, create a host public/private key pair.

2. *Provide Host Public Key to Clients* – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

10.1.0.54 1024 35 156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233765468017262725714134287629413011961955667825956641048695742788814620651941746772984865468615717739390164779355942303577413098022737087794545240839717526463580581767167095748047761172408397175264635805817671670957480477611 7

3. *Import Client's Public Key to the Switch* – Use the **copy tftp public-key** command (Page 4-14) to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch via the User Accounts page as described on page 3-32.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example:

1024 35 134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643 steve@192.168.1.19

4. *Set the Optional Parameters* – On the SSH Settings page, configure the optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. *Enable SSH Service* – On the SSH Settings page, enable the SSH server on the switch.

6. *Challenge-Response Authentication* – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session keyand encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access. The following exchanges take place during this process:

   a. The client sends its public key to the switch.

   b. The switch compares the client's public key to those stored in memory.

   c. If a match is found, the switch uses the public key to encrypt a random sequence of bytes, and sends this string to the client.

 © 2004 Foundry Networks, Inc.

d. The client uses its private key to decrypt the bytes, and sends the decrypted bytes back to the switch.

e. The switch compares the decrypted bytes to the original bytes it sent. If the two sets match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Notes: 1. To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

2. The SSH server supports up to four client sessions. The maximum number

3. of client sessions includes both current Telnet sessions and SSH sessions.

Generating the Host Key Pair

A host public/private key pair is used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client's public key to the switch as described in the proceeding section (Command Usage).

Command Attributes

- **Public-Key of Host-Key** – The public key for the host.

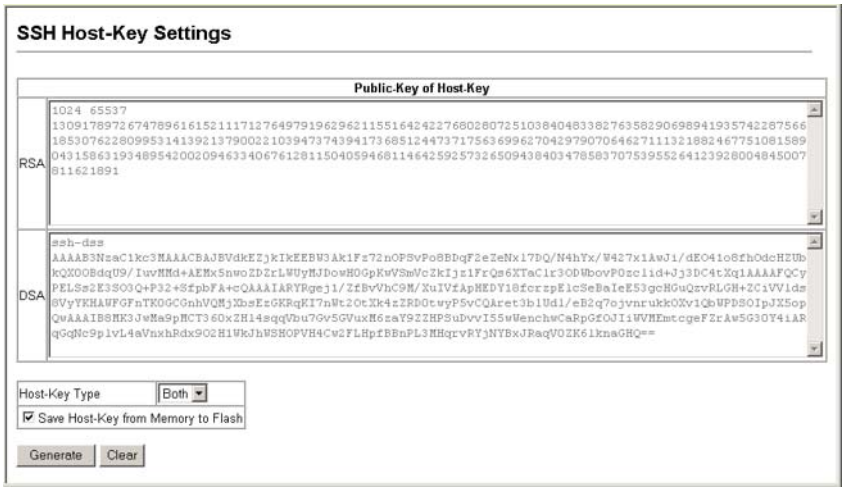
  - RSA: The first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 65537), and the last string is the encoded modulus. - DSA: The first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS). The last string is the encoded modulus.

- **Host-Key Type –** The key type used to generate the host key pair (i.e., public and private keys). (Range: RSA, DSA, Both: Default: RSA) The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

- **Save Host-Key from Memory to Flash –** Saves the host key from RAM (i.e., volatile memory to flash memory. Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair.

 © 2004 Foundry Networks, Inc.

- **Generate –** This button is used to generate the host key pair. Note that you must first generate the host key pair before you can enable the SSH server on the SSH Server Settings page.



CLI – This example generates a host-key pair using both the RSA and DSA algorithms, stores the keys to flash memory, and then displays the host's public keys.

```
Console#ip ssh crypto host-key generate                                    4-35
Console#ip ssh save host-key                                               4-32
Console#show public-key host                                               4-36
Host:
RSA:
1024 65537 12725092254492640213133651454613118967905519236007602865300676182409690947448320102524878965977592168322225584652387791546479807396314033869257931051057652122430528078658854857892726029378660892368414232759121276032591968369705343933643844522333518828717389689451172929051081391964202519093210432857904576489 1
DSA:
ssh-dss AAAAB3NzaC1kc3MAAACBAN6zwIqCqDb3869jYVXlME1sHL0EcE/Re6hlasfEthIwmjhLY4O0jqJZpcEQUgCfYlum0Y2uoLka+Py9ieGWQ8f2gobUZKIICuKg6vjO9XTs7XKc05xfzkBiKviDa+2OrIz6UK+6vFOgvUDFedlnixYTVo+h5v8r0ea2rpnO6DkZAAAAFQCNZn/x17dwpW8RrVDQnSWw4Qk+6QAAAIEAptkGeB6B5hwagH4gUOCY6i1TmrmSiJgfwO9OqRPSMbCAkCC+uzxatOo7drnIZypMx+Sx5RUdMGgKS+9ywsa1cWqHeFY5ilc3lDCNBueeLykZzVS+RS+azTKIk/zrJh8GLGNq375R55yRxFvmcGIn/Q7IphPqyJ3o9MK8LFDfmJEAAACAL8A6tESiswP2OFqX7VGoEbzVDSOIRTMFy3iUXtvGyQAOVSy67Mfc3lMtgqPRUOYXDiwIBp5NXgilCg5z7VqbmRm28mWc5a//f8TUAgPNWKV6W0hqmshQdotVzDR1e+XKNTZj0uTwWfjO5Kytdn4MdoTHgrbl/DMdAfjnte8MZZs=

Console#
```

Configuring the SSH Server

The SSH server includes basic settings for authentication.

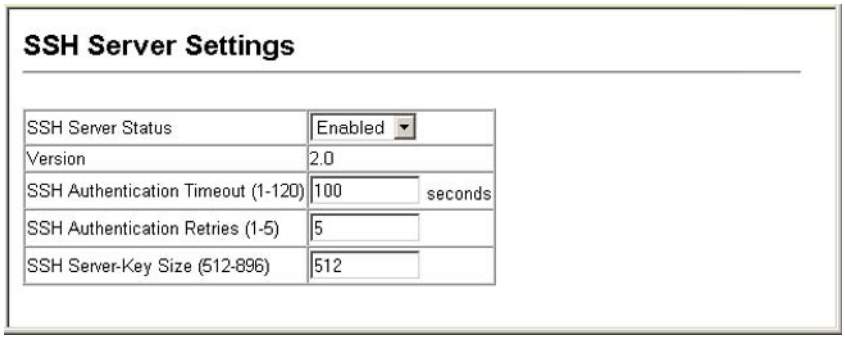
Command Attributes

- **SSH Server Status –** Allows you to enable/disable the SSH server on the switch. (Default: Enabled)
- **Version –** The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access via either SSH Version 1.5 or 2.0 clients.
- **SSH Authentication Timeout –** Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt. (Range: 1 to 120 seconds; Default: 120 seconds)

 © 2004 Foundry Networks, Inc.

- **SSH Authentication Retries –** Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)
- **SSH Server-Key Size –** Specifies the SSH server key size. (Range: 512-896 bits)
  - The server key is a private key that is never shared outside the switch.
  - The host key is shared with the SSH client, and is fixed at 1024 bits.

Web – Click System, SSH Settings. Select Enabled for the SSH Server Status, specify the authentication timeout and number of retries, then click Apply.



CLI – Enter the following commands to configure the SSH service.

```
Console(config)#ip ssh server                                              4-35
Console(config)#ip ssh timeout 100                                         4-35
Console(config)#ip ssh authentication-retries 5                            4-35
Console(config)#
Console#show ip ssh                                                        4-37
Information of secure shell
SSH status: enable
SSH authentication timeout: 100
SSH authentication retries: 5
Console#show ssh                                                           4-36
Connection  Version  State            Username   Encryption
0           2.0      Session-Started  admin      ctos aes128-cbc-hmac-md5
                                                   stoc aes128-cbc-hmac-md5
Console#disconnect ssh 0                                                   4-36
Console#
```

Configuring Port Security

Port security is a feature that allows you to configure a switch port with one or more device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

To use port security, first allow the switch to dynamically learn the <source MAC address, VLAN> pair for frames received on a port for an initial period, and then enable port security to stop address learning. Be sure you enable the learning function long enough to ensure that all valid VLAN members have been registered on the selected port.

 © 2004 Foundry Networks, Inc.

Command Usage

- Note that a secure port has the following restrictions:
  - It should not be connected to a network interconnection device.
  - It cannot be configured as a member of a static trunk.
  - It can be configured as an LACP trunk port, but the switch does not allow the LACP trunk to be enabled.
- A port that is already configured as an LACP or static trunk port cannot be enabled as a secure port.
- The EdgeIron series port security feature allows you to set a maximum number of MAC addresses that can be learned on a port. When port security is enabled, the selected port will stop learning MAC addresses when it has reached the maximum number. The MAC addresses already in the address table will be retained and will not age out. Any other device that attempts to use the port will be prevented from accessing the switch. Note that the EdgeIron 2402CF does not provide an intrusion action to shutdown a port or send an SNMP trap message. The 2402CF also supports a maximum MAC count setting that sets the maximum number of MAC addresses that can be learned on a port when port security is enabled.

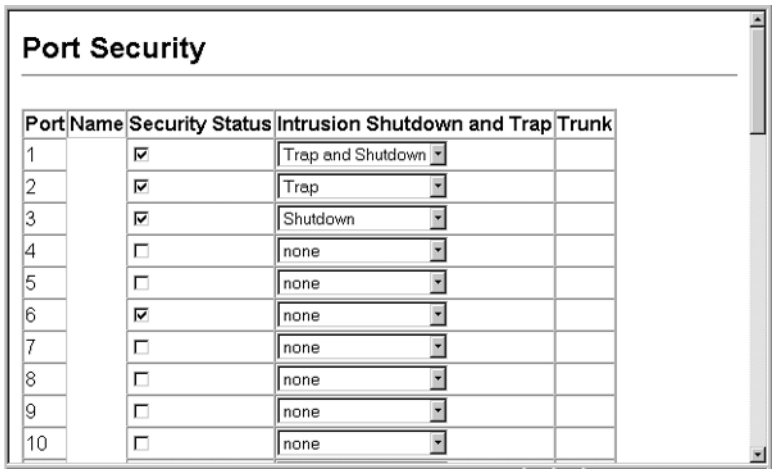
Command Attributes

- **Security Status** – Enables or disables port security on the port. (Default: disabled)
- **Intrusion Shutdown and Trap** – Indicates the action to be taken when a port security violation is detected:
  - **None**: Indicates that no action should be taken. (This is the default.)
  - **Trap**: Indicates that an SNMP trap message only be sent.
  - **Shutdown**: Indicates that the port should only be disabled.
  - **Trap and Shutdown**: Indicates that the port is to be disabled and an SNMP trap message sent.
- **Max MAC Count** – (EdgeIron 2402CF only.) Sets the maximum number of MAC addresses that can be learned on a port when port security is enabled. (Range: 0 - 20, Default: 0)

Note: If a port is disabled (shutdown) due to a security violation, it must be manually re-enabled from the Port/Port Configuration page.

© 2004 Foundry Networks, Inc.

Web – Click Port, Port Security Configuration. Check the checkbox in the Security Status column to enable security for a port, set the security action to be taken when a port intrusion is detected, then click Apply.



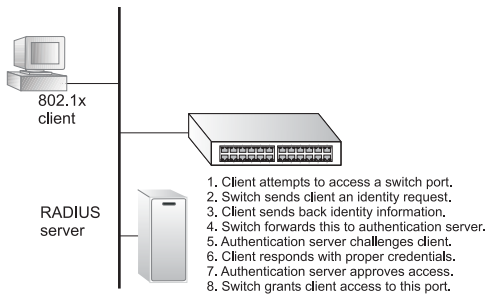
CLI – Use the interface command to select the target port, then use the port security action command to configure the port intrusion action. Use the port security command to enable security for the port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown                    4-114
Console(config-if)#port security max-mac-count 20
Console(config-if)#
```

Configuring 802.1x Port Authentication

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1x (dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.


802.1x
client
RADIUS
server
1. Client attempts to access a switch port.
2. Switch sends client an identity request.
3. Client sends back identity information.
4. Switch forwards this to authentication server.
5. Authentication server challenges client.
6. Client responds with proper credentials.
7. Authentication server approves access.
8. Switch grants client access to this port.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server.

 © 2004 Foundry Networks, Inc.

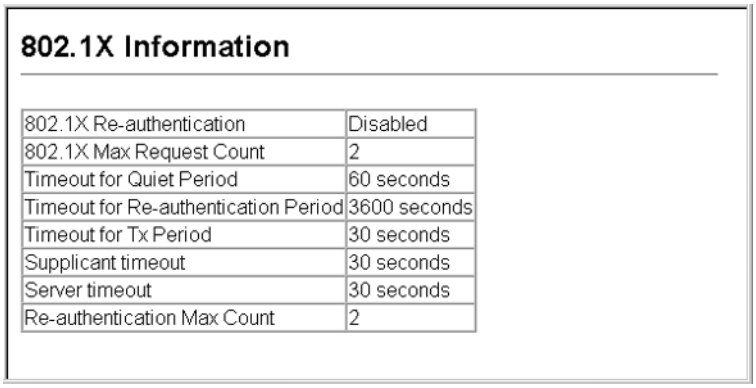
The authentication method can be MD5, TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security), or other. The client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.

Note: TLS, TTLS and PEAP are not currently supported.

The operation of 802.1x on the switch requires the following:

- The switch must have an IP address assigned.
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- Each switch port that will be used must be set to dot1x “Auto” mode.
- Each client that needs to be authenticated must have dot1x client software installed and properly configured.
- The RADIUS server must support EAPOL and MD5 authentication.

Web – Click 802.1x, 802.1x Information.


802.1X Information
802.1X Re-authentication Disabled
802.1X Max Request Count 2
Timeout for Quiet Period 60 seconds
Timeout for Re-authentication Period 3600 seconds
Timeout for Tx Period 30 seconds
Supplicant timeout 30 seconds
Server timeout 30 seconds
Re-authentication Max Count 2

 © 2004 Foundry Networks, Inc.

CLI – This example shows the default protocol settings for dot1x. For a description of the additional entries displayed in the CLI, see “show dot1x” on page 4-66.

```
Console#show dot1x                                          4-66
Global 802.1X Parameters
 reauth-enabled: yes
 reauth-period:  300
 quiet-period:   350
 tx-period:      300
 supp-timeout:   30
 server-timeout: 30
 reauth-max:     2
 max-req:        2

802.1X Port Summary
 Port Name     Status           Mode          Authorized
         1       disabled    ForceAuthorized           n/a
         2       disabled    ForceAuthorized           n/a
.
.
.
        25       disabled    ForceAuthorized           yes
        26        enabled               Auto           yes

802.1X Port Details

802.1X is disabled on port 1
.
.
.

802.1X is enabled on port 26
Max request         2
Quiet period        350
Reauth period       300
Tx period           300
Status              Unauthorized
Port-control        Auto
Supplicant          00-00-00-00-00-00

Authenticator State Machine
State               Connecting
Reauth Count        3
Backend State Machine
State               Idle
Request Count       0
Identifier(Server)  0

Reauthentication State Machine
State               Initialize
Console#
```

Configuring 802.1x Global Settings

The 802.1x protocol includes global parameters that control the client authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server. The configuration options for parameters are described in this section.

Command Attributes

- **802.1X Re-authentication** – Sets the client to be re-authenticated after the interval specified by the Timeout for Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port. (Default: Disabled)

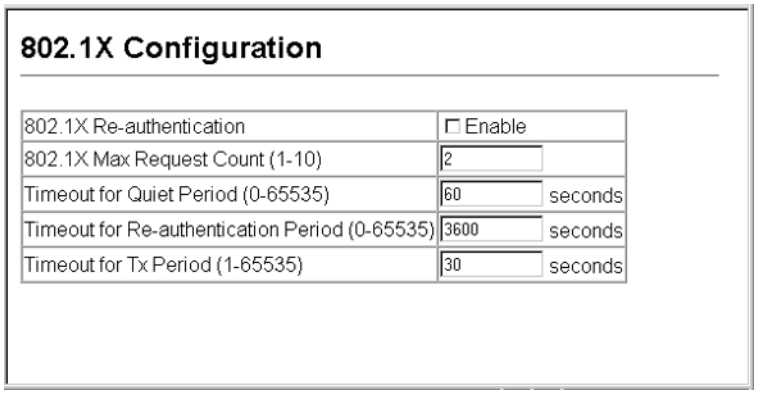
- **802.1X Max Request Count** – Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)

 © 2004 Foundry Networks, Inc.

- **Timeout for Quiet Period** – Sets the time that a switch port waits after the 802.1X Max Request Count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)
- **Timeout for Re-authentication Period** – Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)
- **Timeout for TX Period** – Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)
- **authentication dot1X default*** – Sets the default authentication server type. Note the specified authentication server type must be enabled and properly configured for 802.1x to function properly. (Options: radius).

* CLI only.

Web – Select 802.1X, 802.1X Configuration. Enable dot1x globally for the switch, modify any of the parameters required, and then click Apply.



CLI – This example enables re-authentication and sets all of the global parameters for dot1x.

```
Console(config)#dot1x re-authentication                          4-64
Console(config)#dot1x max-req 5                                  4-63
Console(config)#dot1x timeout quiet-period 40                    4-64
Console(config)#dot1x timeout re-auth 5                          4-65
Console(config)#dot1x timeout tx-period 40                       4-65
Console(config)#authentication dot1x default radius              4-62
Console(config)#
```

Configuring Port Authorization Mode

When dot1x is enabled, you need to specify the dot1x authentication mode configured for each port.

Command Attributes

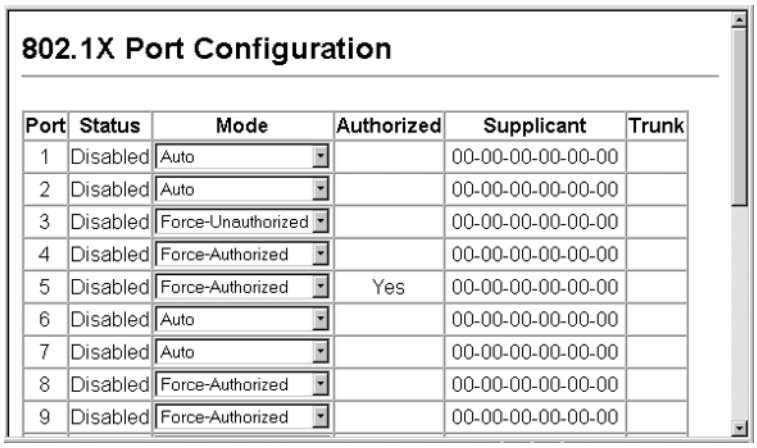
- **Status** – Indicates if authentication is enabled or disabled on the port.
- **Mode** – Sets the authentication mode to one of the following options:
  - **Auto** – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
  - **Force-Authorized** – Forces the port to grant access to all clients, either dot1x-aware or otherwise.

© 2004 Foundry Networks, Inc.

- **Force-Unauthorized** – Forces the port to deny access to all clients, either dot1x-aware or otherwise.

- **Authorized** –
  - **Yes** – Connected client is authorized.
  - **No** – Connected client is not authorized.
  - [*Blank*] – Displays nothing when 802.1x is disabled on a port.
- **Supplicant** – Indicates the MAC address of a connected client.
- **Trunk** – Indicates if the port is configured as a trunk port.

Web – Click 802.1X, 802.1X Port configuration. Select the authentication mode from the drop-down box and click Apply.


802.1X Port Configuration
Port Status Mode Authorized Supplicant Trunk
1 Disabled Auto 00-00-00-00-00-00
2 Disabled Auto 00-00-00-00-00-00
3 Disabled Force-Unauthorized 00-00-00-00-00-00
4 Disabled Force-Authorized 00-00-00-00-00-00
5 Disabled Force-Authorized Yes 00-00-00-00-00-00
6 Disabled Auto 00-00-00-00-00-00
7 Disabled Auto 00-00-00-00-00-00
8 Disabled Force-Authorized 00-00-00-00-00-00
9 Disabled Force-Authorized 00-00-00-00-00-00

CLI – This example sets the authentication mode to enable dot1x on port 2.

```
Console(config)#interface ethernet 1/2                          4-109
Console(config-if)#dot1x port-control auto                      4-63
Console(config-if)#
```

Displaying 802.1x Statistics

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown    4-114
Console(config-if)#port security
Console(config-if)#
```

This switch can display statistics for dot1x protocol exchanges for any port.

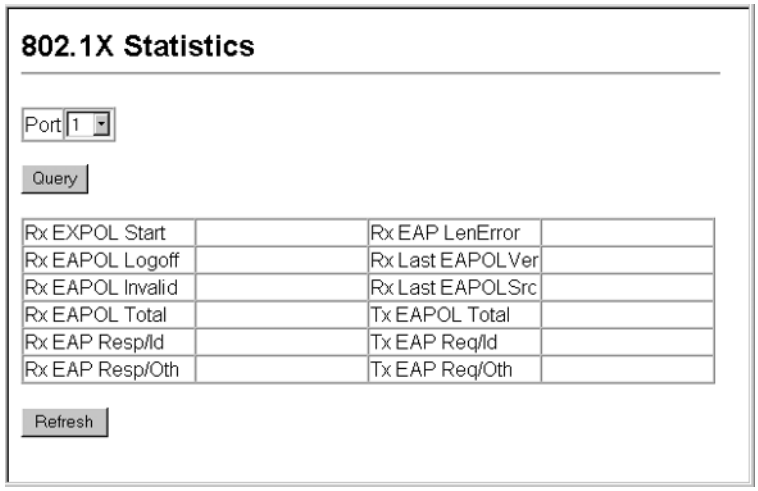
Statistical Values

Parameter	Description
Rx EXPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.

 © 2004 Foundry Networks, Inc.

Parameter	Description
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Rx Last EAPOLVer	The protocol version number carried in the most recently received EAPOL frame.
Rx Last EAPOLSrc	The source MAC address carried in the most recently received EAPOL frame.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.

Web – Select dot1X, dot1X Statistics. Select the required port and then click Query. Click Refresh to update the statistics.



 © 2004 Foundry Networks, Inc.

CLI – This example displays the dot1x statistics for port 4.

```
Console#show dot1x statistics interface ethernet 1/4          4-66

Eth 1/4
Rx: EXPOL      EAPOL      EAPOL      EAPOL      EAP      EAP      EAP
   Start     Logoff    Invalid    Total    Resp/Id  Resp/Oth LenError
       2          0          0       1007      672        0        0

    Last      Last
EAPOLVer     EAPOLSrc
       1     00-00-E8-98-73-21

Tx: EAPOL      EAP      EAP
    Total     Req/Id   Req/Oth
     2017     1005        0
Console#
```

Access Control Lists

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code) or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, specify a mask to modify the precedence in which the rules are checked, and then bind the list to a specific port.

Configuring Access Control Lists

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped; and if no rules match for a list of all deny rules, the packet is accepted.

Command Usage

The following restrictions apply to ACLs:

- Each ACL can have up to 32 rules.
- The maximum number of ACLs is also 32.
- However, due to resource restrictions, the average number of rules bound to the ports should not exceed 20.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.
- The switch does not support the explicit “deny any any” rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.

The order in which active ACLs are checked is as follows:

1. User-defined rules in the Egress MAC ACL for egress ports.
2. User-defined rules in the Egress IP ACL for egress ports.

 © 2004 Foundry Networks, Inc.

3. User-defined rules in the Ingress MAC ACL for ingress ports.
4. User-defined rules in the Ingress IP ACL for ingress ports.
5. Explicit default rule (permit any any) in the ingress IP ACL for ingress ports.
6. Explicit default rule (permit any any) in the ingress MAC ACL for ingress ports.
7. If no explicit rule is matched, the implicit default is permit all.

Setting the ACL Name and Type

Use the ACL Configuration page to designate the name and type of an ACL.

Command Attributes

- **Name** – Name of the ACL. (Maximum length: 16 characters)
- **Type** – There are three filtering modes:
  - **Standard**: IP ACL mode that filters packets based on the source IP address.
  - **Extended**: IP ACL mode that filters packets based on source or destination IP address, as well as protocol type and protocol port number. If the “TCP” protocol is specified, then you can also filter packets based on the TCP control code.
  - **MAC**: MAC ACL mode that filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

Web – Click Security, ACL, ACL Configuration. Enter an ACL name in the Name field, select the list type (IP Standard, IP Extended, or MAC), and click Add to open the configuration page for the new list.



CLI – This example creates a standard IP ACL named bill.

```
Console(config)#access-list ip standard bill                    4-70
Console(config-std-acl)#
```

Configuring a Standard IP ACL

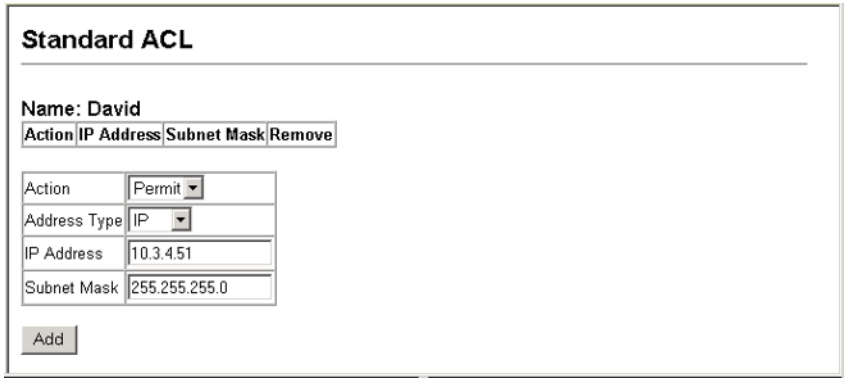
Command Attributes

- **Action** – An ACL can contain permit rules, deny rules, or a combination of both. (Default: Permit rules)
- **Address Type** - Specifies the filter type - Any, Host, or IP. (Default: Any)

 © 2004 Foundry Networks, Inc.

- **IP Address** – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)
- **Subnet Mask** – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Web – Specify the action (i.e., Permit or Deny). Select the address type (Any, Host, or IP). If you select “Host,” enter a specific address. If you select “IP,” enter a subnet address and the mask for an address range. Then click Add.



CLI – This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21                    4-70
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Configuring an Extended IP ACL

Command Attributes

- **Action** – An ACL can contain permit rules, deny rules or a combination of both. (Default: Permit rules)
- **Source Address Type** – Specifies the filter type - Any, Host, or IP. (Default: Any)
- **Source/Destination IP** – Specifies the source or destination IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)
- **Source/Destination Subnet Mask** – Subnet mask for source or destination address. (See the description for SubMask on page 33-41.)
- **Service Type** – Packet priority settings based on the following criteria:
- **Precedence** – IP precedence level. (Range: 0-7)
- **TOS** – Type of Service level. (Range: 0-15)

 © 2004 Foundry Networks, Inc.

- **DSCP** – DSCP priority level. (Range: 0-64)
- **Protocol** – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: TCP)
- **Source/Destination Port** – Source/destination port number for the specified protocol type. (Range: 0-65535)
- **Source/Destination Port Bitmask** – Decimal number representing the port bits to match. (Range: 0-65535)
- **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- **Control Code Bitmask** – Decimal number representing the code bits to match.

  The control bitmask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:

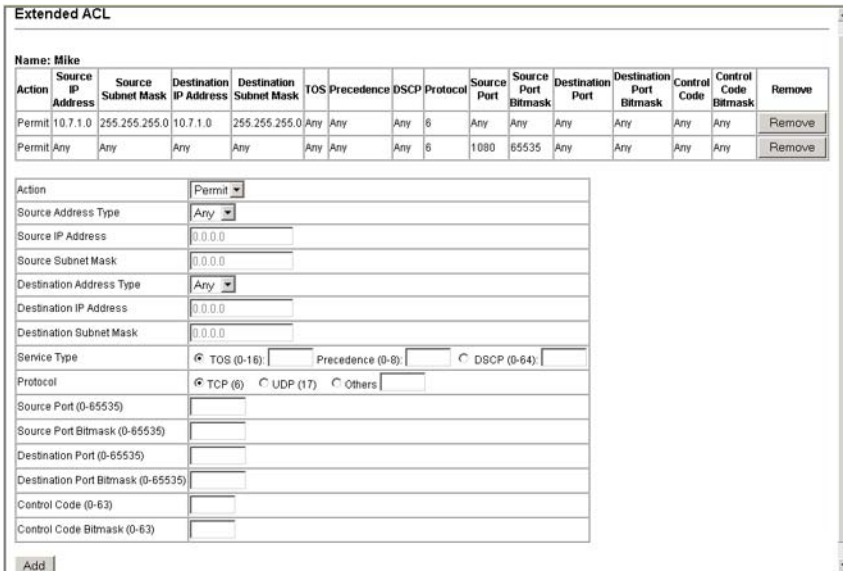
  - 1 (fin) – Finish
  - 2 (syn) – Synchronize
  - 4 (rst) – Reset
  - 8 (psh) – Push
  - 16 (ack) – Acknowledgement
  - 32 (urg) – Urgent pointer

  For example, use the code value and mask below to catch packets with the following flags set:

  - SYN flag valid, use control-code 2, control bitmask 2
  - Both SYN and ACK valid, use control-code 18, control bitmask 18
  - SYN valid and ACK invalid, use control-code 2, control bitmask 18

 © 2004 Foundry Networks, Inc.

Web – Specify the action (i.e., Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or IP). If you select “Host,” enter a specific address. If you select “IP,” enter a subnet address and the mask for an address range. Set any other required criteria, such as service type, protocol type, or TCP control code. Then click Add.



CLI – This example adds three rules:

1. Accept any incoming packets if the source address is in subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

2. Allow TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

3. Permit all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to “SYN.”

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any      4-71
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any dport
   80
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any tcp
   control-code 2 2
Console(config-std-acl)#
```

Configuring a MAC ACL

Command Attributes

- **Action** – An ACL can contain permit rules, deny rules, or a combination of both. (Default: Permit rules)

- **Source/Destination Address Type** – Use “Any” to include all possible addresses, “Host” to indicate a specific MAC address, or “MAC” to specify an address range with the Address and Bitmask fields. (Options: Any, Host, MAC; Default: Any)

 © 2004 Foundry Networks, Inc.

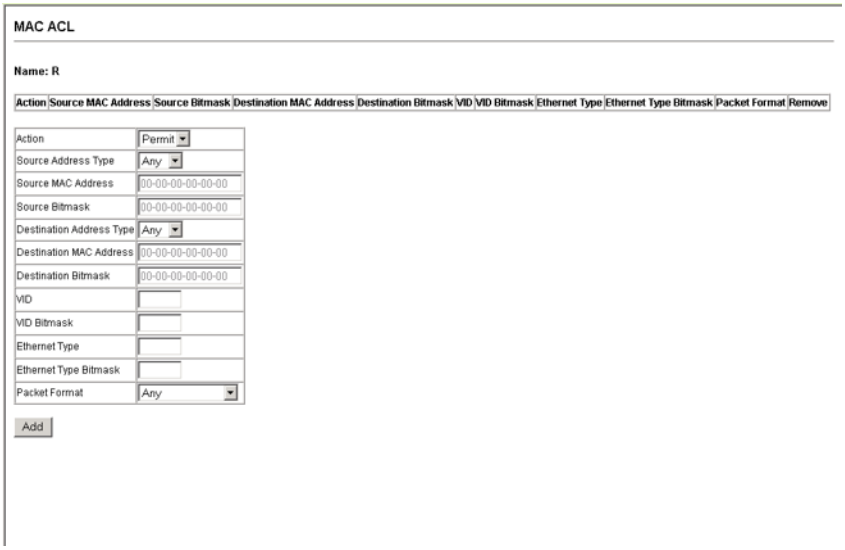
- **Source/Destination MAC Address** – Source or destination MAC address.
- **Source/Destination Bitmask** – Hexidecimal mask for source or destination MAC address.
- **VID** – VLAN ID. (Range: 1-4095)
- **VID Mask** – VLAN bitmask. (Range: 1-4095)
- **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 600-fff hex.)

  A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).
- **Ethernet Type Bitmask** – Protocol bitmask. (Range: 600-fff hex.)
- **Packet Format** – This attribute includes the following packet types:
  - **Any** – Any Ethernet packet type.
  - **Untagged-eth2** – Untagged Ethernet II packets.
  - **Untagged-802.3** – Untagged Ethernet 802.3 packets.
  - **Tagged-eth2** – Tagged Ethernet II packets.
  - **Tagged-802.3** – Tagged Ethernet 802.3 packets.

Command Usage

- Egress MAC ACLs only work for destination-mac-known packets, not for multicast, broadcast, or destination-mac-unknown packets.

Web – Specify the action (i.e., Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or MAC). If you select “Host,” enter a specific address (e.g., 11-22-33-44-55-66). If you select “MAC,” enter a base address and a hexidecimal bitmask for an address range. Set any other required criteria, such as VID, Ethernet type, or packet format. Then click Add.



 © 2004 Foundry Networks, Inc.

CLI – This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de
   ethertype 0800                                          4-81
Console(config-mac-acl)#
```

Configuring ACL Masks

You can specify optional masks that control the order in which ACL rules are checked. The switch includes two system default masks that pass/filter packets matching the permit/deny rules specified in an ingress ACL. You can also configure up to seven user-defined masks for an ingress or egress ACL. A mask must be bound exclusively to one of the basic ACL types (i.e., Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL), but a mask can be bound to up to four ACLs of the same type.

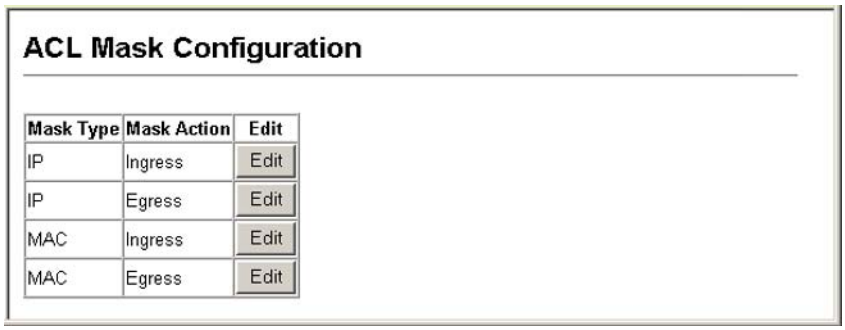
Command Usage

- Up to seven entries can be assigned to an ACL mask.
- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules are entered.
- First create the required ACLs and the ingress or egress masks before mapping an ACL to an interface.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.

Specifying the Mask Type

Use the ACL Mask Configuration page to edit the mask for the Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL.

Web – Click Security, ACL, ACL Mask Configuration. Click Edit for one of the basic mask types to open the configuration page.



 © 2004 Foundry Networks, Inc.

CLI – This example creates an IP ingress mask, and then adds two rules. Each rule is checked in order of precedence to look for a match in the ACL entries. The first entry matching a mask is applied to the inbound packet.

```
Console(config)#access-list ip mask-precedence in              4-73
Console(config-ip-mask-acl)#mask host any                      4-74
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

Configuring an IP ACL Mask

This mask defines the fields to check in the IP header.

Command Usage

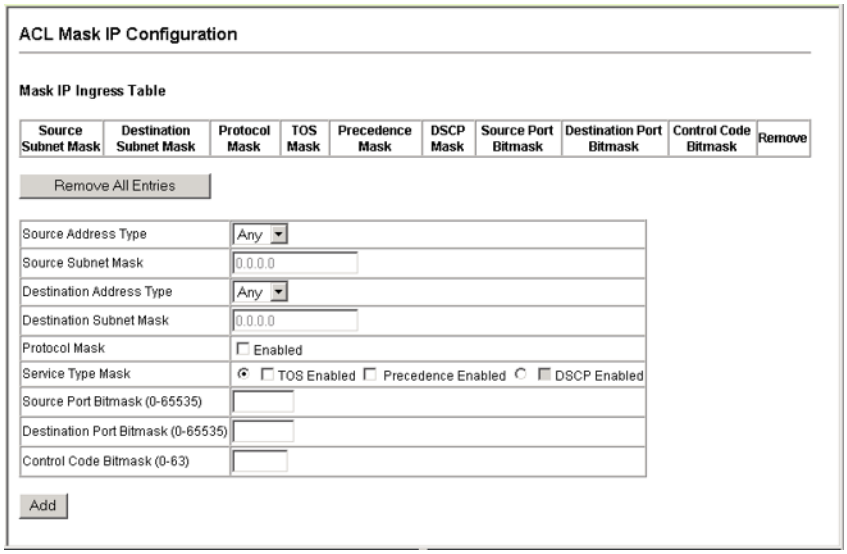
- Masks that include an entry for a Layer 4 protocol source port or destination port can only be applied to packets with a header length of exactly five bytes.

Command Attributes

- **Source/Destination Address Type** – Use “Any” to include all possible addresses, “Host” to indicate a specific MAC address, or “MAC” to specify an address range with the Address and Bitmask fields. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination Subnet Mask** – Subnet mask for source or destination address. (See the description for SubMask on page 33-41.)
- **Protocol Mask** – Check the protocol field.
- **Service Type Mask** – Check the rule for the specified priority type. (Options: Precedence, TOS, DSCP; Default: TOS)
- **Source/Destination Port Bitmask** – Protocol port of rule must match this bitmask. (Range: 0-65535)
- **Control Bitmask** – Control flags of rule must match this bitmask. (Range: 0-63)

© 2004 Foundry Networks, Inc.

Web – Configure the mask to match the required rules in the IP ingress or egress ACLs. Set the mask to check for any source or destination address, a specific host address, or an address range. Include other criteria to search for in the rules, such as a protocol type or one of the service types. Or use a bitmask to search for specific protocol port(s) or TCP control code(s). Then click Add.



CLI – This shows that the entries in the mask override the precedence in which the rules are entered into the ACL. In the following example, packets with the source address 10.1.1.1 are dropped because the “deny 10.1.1.1 255.255.255.255” rule has the higher precedence according the “mask host any” entry.

```
Console(config)#access-list ip standard A2                    4-70
Console(config-std-acl)#permit 10.1.1.0 255.255.255.0         4-70
Console(config-std-acl)#deny 10.1.1.1 255.255.255.255
Console(config-std-acl)#exit
Console(config)#access-list ip mask-precedence in             4-73
Console(config-ip-mask-acl)#mask host any                     4-74
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

Configuring a MAC ACL Mask

This mask defines the fields to check in the packet header.

Command Usage

You must configure a mask for an ACL rule before you can bind it to a port.

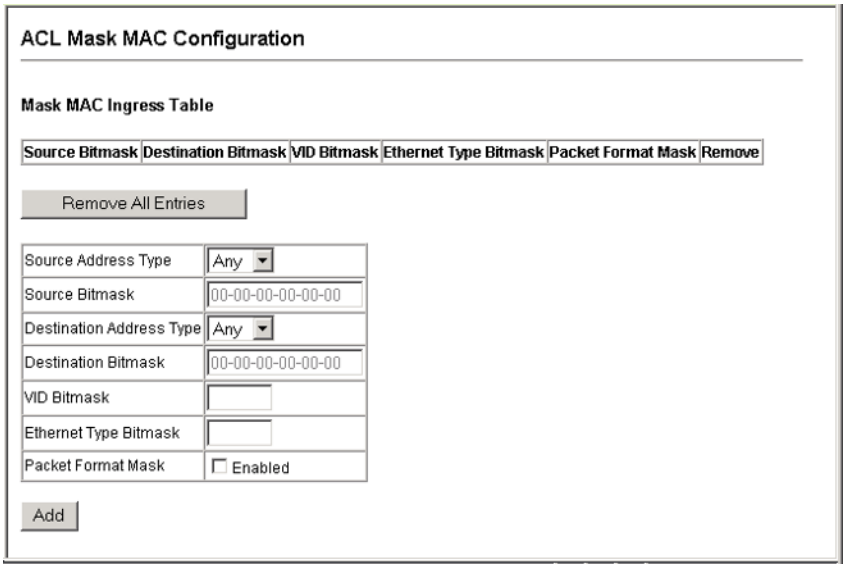
Command Attributes

- **Source/Destination Address Type** – Use “Any” to match any address, “Host” to specify the host address for a single node, or “MAC” to specify a range of addresses. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination Bitmask** – Address of rule must match this bitmask.
- **VID Bitmask** – VLAN ID of rule must match this bitmask.

 © 2004 Foundry Networks, Inc.

- **Ethernet Type Bitmask** – Ethernet type of rule must match this bitmask.
- **Packet Format Bitmask** – A packet format must be specified in the rule.

Web – Configure the mask to match the required rules in the MAC ingress or egress ACLs. Set the mask to check for any source or destination address, a host address, or an address range. Use a bitmask to search for specific VLAN ID(s) or Ethernet type(s). Or check for rules where a packet format was specified. Then click Add.



CLI – This example shows how to create an Ingress MAC ACL and bind it to a port. You can then see that the order of the rules have been changed by the mask.

```
Console(config)#access-list mac M4                              4-81
Console(config-mac-acl)#permit any any                          4-81
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11 ff-ff-ff-
   ff-ff-ff any vid 3                                           4-81
Console(config-mac-acl)#end
Console#show access-list                                        4-90
MAC access-list M4:
  permit any any
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
Console(config)#access-list mac mask-precedence in              4-83
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any
   vid                                                          4-84
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/12                         4-109
Console(config-if)#mac access-group M4 in                       4-84
Console(config-if)#end
Console#show access-list
MAC access-list M4:
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
  permit any any
MAC ingress mask ACL:
  mask pktformat host any vid
Console#
```

Binding a Port to an Access Control List

After configuring the Access Control Lists (ACL), you can bind the ports that need to filter traffic to the appropriate ACLs. You can only bind a port to one ACL for each basic type – IP ingress, IP egress, MAC ingress and MAC egress.

 © 2004 Foundry Networks, Inc.

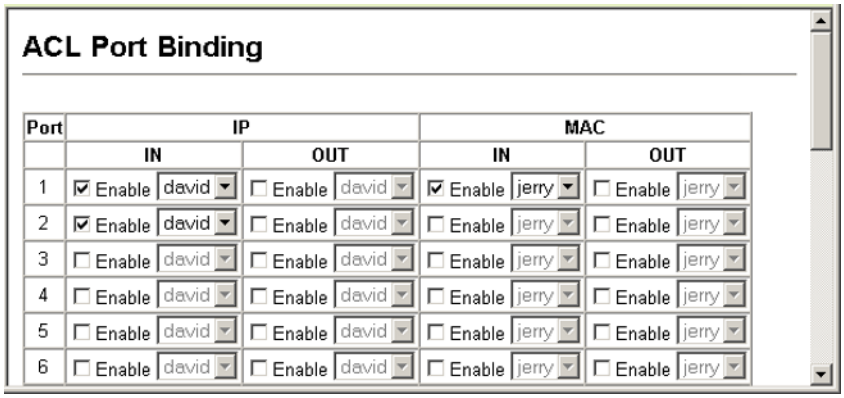
Command Usage

- This switch supports ACLs for both ingress and egress filtering. However, you can only bind one IP ACL and one MAC ACL to any port for ingress filtering, and one IP ACL and one MAC ACL to any port for egress filtering. In other words, only four ACLs can be bound to an interface – Ingress IP ACL, Egress IP ACL, Ingress MAC ACL and Egress MAC ACL.
- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.
- The switch does not support the explicit “deny any any” rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in the ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.

Command Attributes

- Port – Fixed port or SFP module. (Range: 1-24)
- **IP** – Specifies the IP ACL to bind to a port.
- **MAC** – Specifies the MAC ACL to bind to a port.
- **IN** – ACL for ingress packets.
- **OUT** – ACL for egress packets.
- *ACL Name* – Name of the ACL.

Web – Click ACL, ACL Port Binding. Mark the Enable field for the port you want to bind to an ACL for ingress or egress traffic, select the required ACL from the drop-down list, then click Apply.


ACL Port Binding
Port
IP
MAC
IN
OUT
IN
OUT
1 Enable david Enable david Enable jerry Enable jerry
2 Enable david Enable david Enable jerry Enable jerry
3 Enable david Enable david Enable jerry Enable jerry
4 Enable david Enable david Enable jerry Enable jerry
5 Enable david Enable david Enable jerry Enable jerry
6 Enable david Enable david Enable jerry Enable jerry

CLI – This example assigns an IP and MAC ingress ACL to port 1, and an IP ingress ACL to port 2.

```
Console(config)#interface ethernet 1/1                          4-109
Console(config-if)#ip access-group david in                     4-77
Console(config-if)#mac access-group jerry in                    4-87
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
```

 © 2004 Foundry Networks, Inc.

Filtering IP Addresses for Management Access

You can specify the client IP addresses that are allowed management access to the switch through the web interface, SNMP, or Telnet.

Command Usage

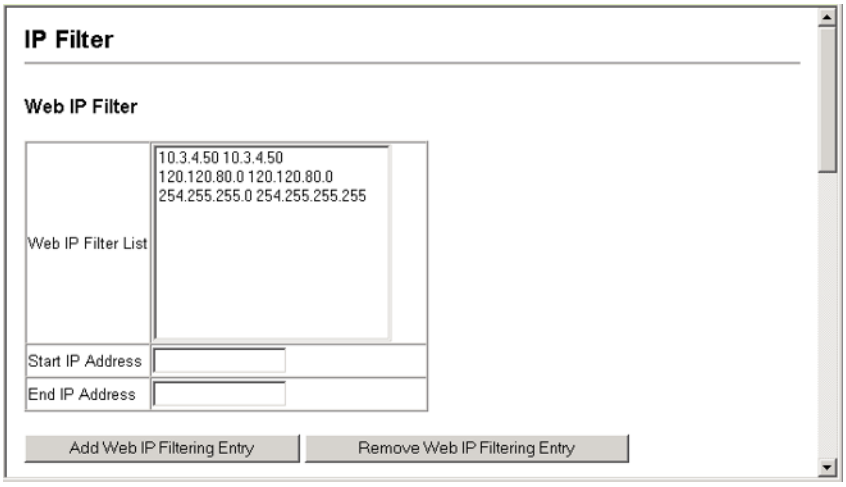
- The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.
- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP addresses can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Command Attributes

- Web IP Filter – Configures IP address(es) for the web group.
- SNMP IP Filter – Configures IP address(es) for the SNMP group.
- Telnet IP Filter – Configures IP address(es) for the Telnet group.
- IP Filter List – IP addresses that are allowed management access to this interface.
- Start IP Address – A single IP address, or the starting address of a range.
- End IP Address – The end address of a range.

© 2004 Foundry Networks, Inc.

Web – Click Security, IP Filter. Enter the addresses that are allowed management access to an interface, and click Add IP Filtering Entry.



CLI – This example restricts management access for Telnet and SNMP clients.

```
Console(config)#management telnet-client 192.168.1.19          4-22
Console(config)#management telnet-client 192.168.1.25 192.168.1.30
Console(config)#management snmp-client 10.1.2.3 255.255.255.2554-22
Console(config)#end
Console#sh management telnet-client                             4-23
Management IP Filter
 TELNET-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30
Console#sh management snmp-client                             4-23
Management IP Filter
 SNMP-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 10.1.2.3              255.255.255.255
Console#
```

Port Configuration

Displaying Connection Status

You can use the Port Information or Trunk Information pages to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

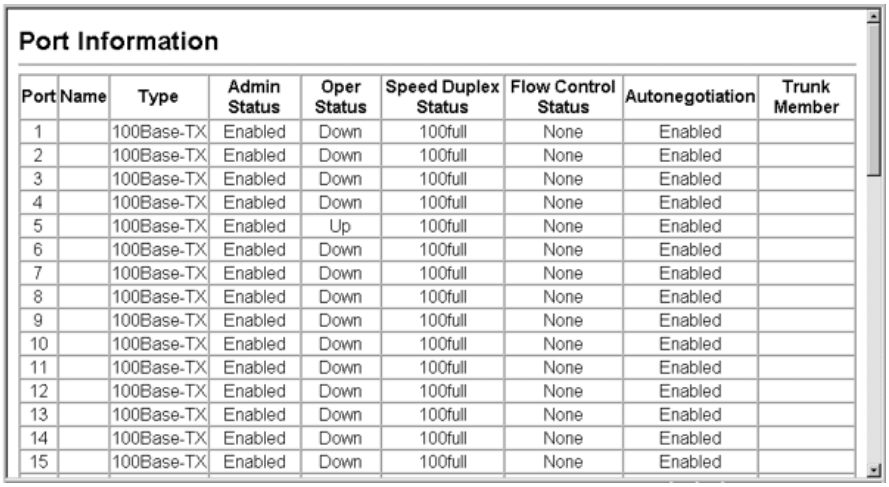
Command Attributes

- **Name** – Interface label.
- **Type** – Indicates the of port type (100Base-TX, 1000Base-TX or 1000Base-SFP).
- **Admin Status** – Shows if the interface is enabled or disabled.
- **Oper Status** – Indicates if the link is Up or Down.

 © 2004 Foundry Networks, Inc.

- **Speed/Duplex Status** – Shows the current speed and duplex mode.
- **Flow Control Status** – Indicates the type of flow control currently in use.
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Trunk Member** – Shows if port is a trunk member. (Port Information only.)
- **Creation** – Shows if a trunk is manually configured or dynamically set via LACP. (Trunk Information only.)

Web – Click Port, Port Information or Trunk Information. Modify the required interface settings, and click Apply.



Port Information

Port	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Trunk Member
1		100Base-TX	Enabled	Down	100full	None	Enabled	
2		100Base-TX	Enabled	Down	100full	None	Enabled	
3		100Base-TX	Enabled	Down	100full	None	Enabled	
4		100Base-TX	Enabled	Down	100full	None	Enabled	
5		100Base-TX	Enabled	Up	100full	None	Enabled	
6		100Base-TX	Enabled	Down	100full	None	Enabled	
7		100Base-TX	Enabled	Down	100full	None	Enabled	
8		100Base-TX	Enabled	Down	100full	None	Enabled	
9		100Base-TX	Enabled	Down	100full	None	Enabled	
10		100Base-TX	Enabled	Down	100full	None	Enabled	
11		100Base-TX	Enabled	Down	100full	None	Enabled	
12		100Base-TX	Enabled	Down	100full	None	Enabled	
13		100Base-TX	Enabled	Down	100full	None	Enabled	
14		100Base-TX	Enabled	Down	100full	None	Enabled	
15		100Base-TX	Enabled	Down	100full	None	Enabled	

CLI – This example shows the connection status for Port 13.

```
Console#show interfaces status ethernet 1/13                    4-117
Information of Eth 1/13
 Basic information:
  Port type: 1000T
  Mac address: 00-04-80-BD-47-4E
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Broadcast storm: Enabled
  Broadcast storm limit: 500 packets/second
  Flow control: Disabled
  Lacp: Disabled
  Port security: Disabled
  Max MAC count: 0
  Port security action: None
  Combo forced mode: None
 Current status:
  Link status: Down
  Operation speed-duplex: 1000full
  Flow control type: None
Console#
```

 © 2004 Foundry Networks, Inc.

Configuring Interface Connections

You can use the Trunk Configuration or Port Configuration page to enable/disable an interface, manually fix the speed and duplex mode, set flow control, set auto-negotiation, and set the interface capabilities to advertise.

Command Attributes

- **Name** – Allows you to label an interface. (Range: 1-64 characters)
- **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also disable an interface for security reasons.
- **Speed/Duplex** – Allows manual selection of port speed and duplex mode (i.e., with auto-negotiation disabled).
- **Flow Control** – Allows automatic or manual selection of flow control.
- **Autonegotiation/Port Capabilities** – Allows auto-negotiation to be enabled/disabled. Specifies the capabilities to be advertised for a port during auto-negotiation. The following capabilities are supported.

  - **10half** - Supports 10 Mbps half-duplex operation
  - **10full** - Supports 10 Mbps full-duplex operation
  - **100half** - Supports 100 Mbps half-duplex operation
  - **100full** - Supports 100 Mbps full-duplex operation
  - **1000full** - Supports 1000 Mbps full-duplex operation
  - **Sym** (Gigabit only) - Check this item to transmit and receive pause frames, or clear it to auto-negotiate the sender and receiver for asymmetric pause frames. (The current switch chip only supports symmetric pause frames.)
  - **FC** - Supports flow control
    Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation. (Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.)

    Default: Auto-negotiation enabled; Advertised capabilities for 100BASE-TX – 10half, 10full, 100half, 100full; 1000BASE-T – 10half, 10full, 100half, 100full, 1000full; 1000BASE-SX/LX/LH – 1000full)

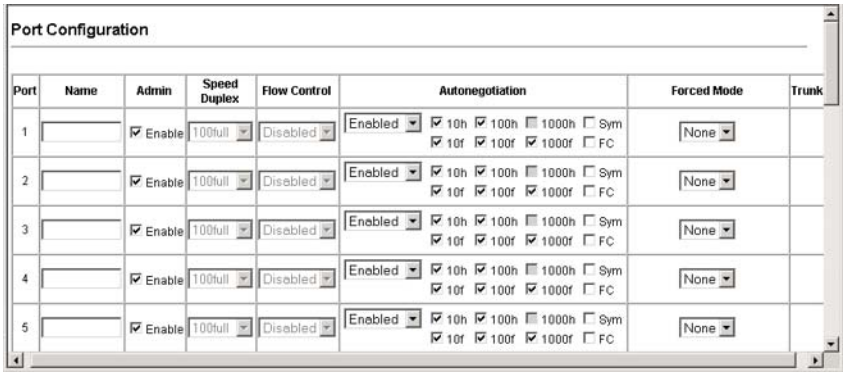
Note: Due to a hardware limitation, flow control only works on those ports located in the same chip (ports 1-24, 49 and ports 25-48, 50). Cross-chip flow control does not work.

- **Forced Mode** – Indicates if a port or trunk has been set to forced mode.
- **Trunk** – Indicates if a port is a member of a trunk. To create trunks and select port members, see “Multicast Configuration” on page 3-114.

 © 2004 Foundry Networks, Inc.

Note: Auto-negotiation must be disabled before you can configure or force the interface to use the Speed/Duplex Mode or Flow Control options.

Web – Click Port, Port Configuration or Trunk Configuration. Modify the required interface settings, and click Apply.



CLI – Select the interface, and then enter the required settings.

```
Console(config)#interface ethernet 1/13                    4-109
Console(config-if)#description RD SW#13                    4-109
Console(config-if)#shutdown                                4-113
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation                          4-110
Console(config-if)#speed-duplex 100half                    4-110
Console(config-if)#flowcontrol                             4-112
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half                    4-111
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
```

Statically Configuring a Trunk

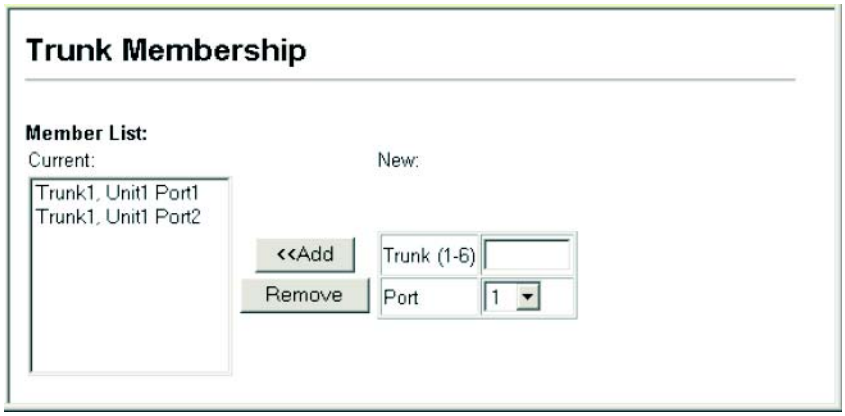
Command Usage

When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation. Static trunks have to be manually configured at both ends of the link.

- To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.

 © 2004 Foundry Networks, Inc.

Web – Click Port, Trunk Membership. Enter a trunk ID of 1-6 in the Trunk field, select any of the switch ports from the scroll-down port list, and click Add. After you have completed adding ports to the member list, click Apply



Dynamically Configuring a Trunk

Ports can be combined into an aggregate link to increase the bandwidth of a network connection where bottlenecks exist or to ensure fault recovery. You can create up to six trunks at a time, with any single trunk containing up to four ports.

Model Name	Trunk Load Balance Selection Criterion
EIF 2402CF, EIF 4802CF	L2 Src and Dst MAC address
EIF 24G	L2 Src MAC, L2 Dst MAC, L2 ether type, L2 vlan ID, IP multicast Src MAC, IP multicast Dst MAC
EIF 24G-A, EIF-48G	L2 Src and Dst MAC address

Command Usage

Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the Web interface or CLI to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- The maximum number of ports that can be combined as a static trunk:
  - EdgeIron 4802CF, 2402CF: Four 10/100 Mbps ports, and two 1000 Mbps ports. (Total: 6 ports)
  - EdgeIron 24G-A, 24G, 48G: Six 1000 Mbps ports.
- The ports at both ends of a connection must be configured as trunk ports.
- Static trunkshave to be manually configured at both ends of the link
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.

© 2004 Foundry Networks, Inc.

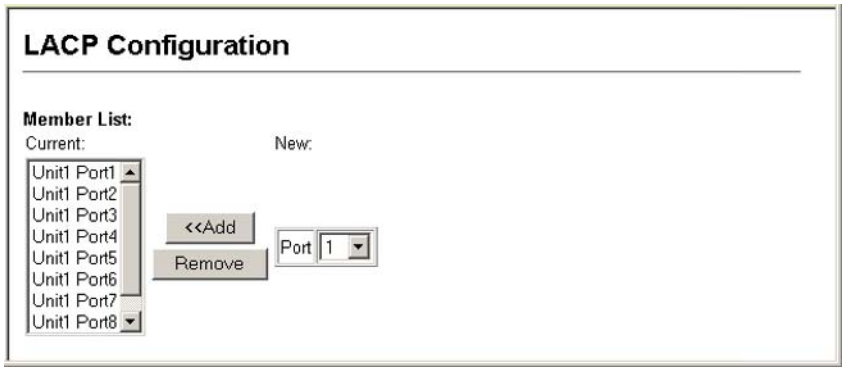
- All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

Enabling LACP on Selected Ports

Command Usage

To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP. If the target switch has also enabled LACP on th connected ports, the trunk will be activate automatically. A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID. If more than four ports attached to the same targe switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails. All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.

Web – Click Port, LACP, Configuration. Select any of the switch ports from the scroll-down port list and click Add. After you have completed adding ports to the member list, click Apply.



© 2004 Foundry Networks, Inc.

CLI – The following example enables LACP for ports 1 to 6. Just connect these ports to LACP-enabled trunk ports on another switch to form a trunk.

```
Console(config)#interface ethernet 1/1                4-109
Console(config-if)#lacp                                      4-178
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1         4-117
Information of Trunk
 Basic information:
  Port type: 1000T
  Mac address: 22-22-22-22-22-2d
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control status: Disabled
  Port security: Disabled
  Max MAC count: 0
  Port security action: None
  Combo forced mode: None
 Current status:
  Created by: Lacp
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6,
Console#
```

Configuring LACP Parameters

Dynamically Creating a Port Channel

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP System Priority.
- Ports must have the same LACP port Admin Key.
- However, if the “port channel” Admin Key is set (page 4-142), then the port Admin Key must be set to the same value for a port to be allowed to join a channel group.

Note: If the port channel admin key (lacp admin key, page 44-181) is not set (through the CLI) when a channel group is formed (i.e., it has a null value of 0), this key is set to the same value as the port admin key used by the interfaces that joined the group (lacp admin key, as described in this section and on page 44-181).

Note: The maximum number of ports in a trunk is 8, and the maximum number of trunk groups is 12. There is no limitation on the number of LACP members.

 © 2004 Foundry Networks, Inc.

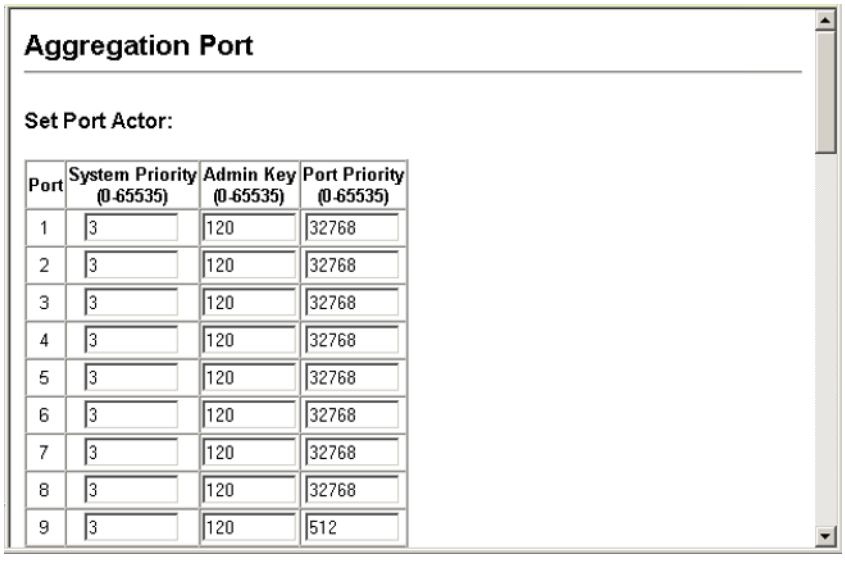
Command Attributes

Set Port Actor – This menu sets the local side of an aggregate link; i.e., the ports on this switch.

- **Port** – Port number. (Range: 1-24)
- **System Priority** – LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535; Default: 32768)
  - Ports must be configured with the same system priority to join the same LAG.
  - System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- **Admin Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default: 0)
- **Port Priority** – If a link goes down, LACP port priority is used to select a backup link. (Range: 0-65535; Default: 32768)

Set Port Partner – This menu sets the remote side of an aggregate link; i.e., the ports on the attached device. The command attributes have the same meaning as those used for the port actor. However, configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Web – Click Port, LACP, Aggregation Port. Set the System Priority, Admin Key, and Port Priority for the Port Actor. You can optionally configure these settings for the Port Partner. (Be aware that these settings only affect the administrative state of the partner, and will not take effect until the next time an aggregate link is formed with this device.) After you have completed setting the port LACP parameters, click Apply.



 © 2004 Foundry Networks, Inc.

CLI – The following example configures LACP parameters for ports 1-6. Ports 1-4 are used as active members of the LAG; ports 5 and 6 are set to backup mode.

```
Console(config)#interface ethernet 1/1                    4-109
Console(config-if)#lacp actor system-priority 3           4-178
Console(config-if)#lacp actor admin-key 120               4-180
Console(config-if)#lacp actor port-priority 128           4-181
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#lacp actor system-priority 3
Console(config-if)#lacp actor admin-key 120
Console(config-if)#lacp actor port-priority 512
Console(config-if)#end
Console#sh lacp sysid                                     4-182
Channel Group    System Priority    System MAC Address
--------------------------------------------------------------------
            1              32768     00-00-E9-31-31-31
            2              32768     00-00-E9-31-31-31
            3              32768     00-00-E9-31-31-31
            4              32768     00-00-E9-31-31-31
            5              32768     00-00-E9-31-31-31
            6              32768     00-00-E9-31-31-31
Console#show lacp 1 internal                         4-182
Channel group : 1
--------------------------------------------------------------------
Oper Key : 120
Admin Key : 120
Console#
```

Displaying LACP Port Counters

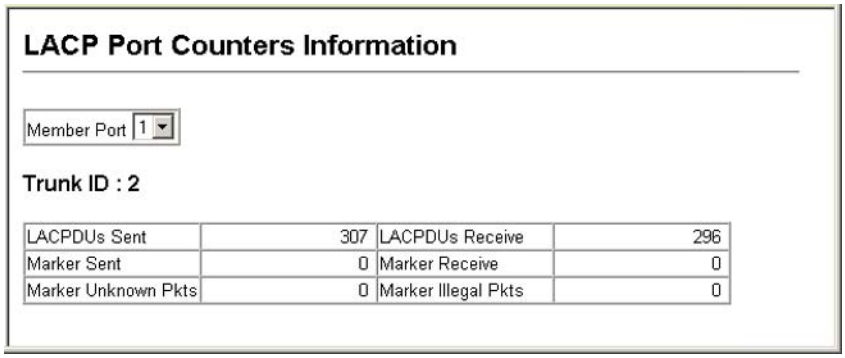
You can display statistics for LACP protocol messages.

Counter Information

Parameter	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
LACPDUs Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
LACPDUs Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

 © 2004 Foundry Networks, Inc.

Web – Click Port, LACP, Port Counters Information. Select a member port to display the corresponding information.



CLI – The following example displays LACP counters for port channel 1.

```
Console#show 1 lacp counters                                    4-182
Channel group : 1 ------------------------------------------------
Eth 1/ 1 ---------------------------------------------------------
  LACPDUs Sent : 21
  LACPDUs Received : 21
  Marker Sent : 0
  Marker Received : 0
  LACPDUs Unknown Pkts : 0
  LACPDUs Illegal Pkts : 0
:
Console#
```

Displaying LACP Settings and Status for the Local Side

You can display configuration settings and the operational state for the local side of an link aggregation.

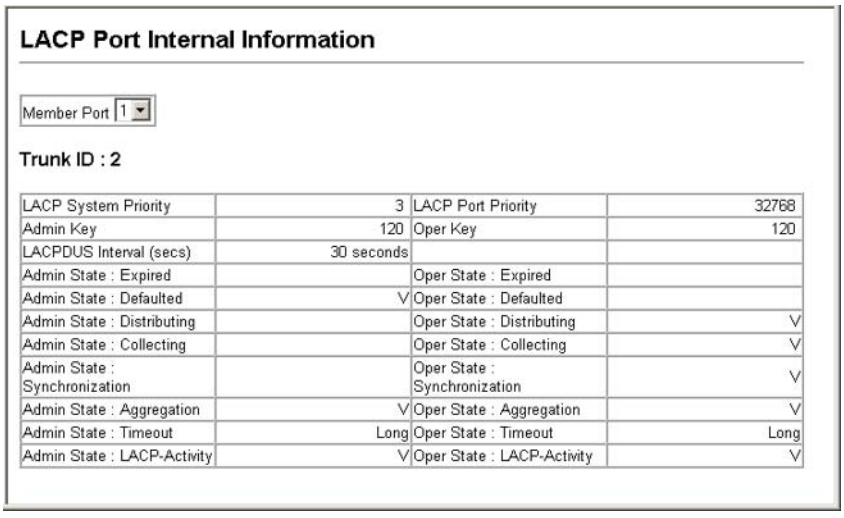
Internal Configuration Information

Parameter	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
LACP System Priority	LACP system priority assigned to this port channel.

© 2004 Foundry Networks, Inc.

Parameter	Description
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: Expired – The actor's receive machine is in the expired state; Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

Web – Click Port, LACP, Port Internal Information. Select a port channel to display the corresponding information.


LACP Port Internal Information
Member Port 1
Trunk ID : 2
LACP System Priority 3 LACP Port Priority 32768
Admin Key 120 Oper Key 120
LACPDUS Interval (secs) 30 seconds
Admin State : Expired Oper State : Expired
Admin State : Defaulted V Oper State : Defaulted
Admin State : Distributing Oper State : Distributing V
Admin State : Collecting Oper State : Collecting V
Admin State : Synchronization Oper State : Synchronization V
Admin State : Aggregation V Oper State : Aggregation V
Admin State : Timeout Long Oper State : Timeout Long
Admin State : LACP-Activity V Oper State : LACP-Activity V

 © 2004 Foundry Networks, Inc.

CLI – The following example displays the LACP configuration settings and operational state for the local side of port channel 1.

```
Console#show 1 lacp internal                                    4-182
Channel group : 1
------------------------------------------------------------------------
Oper Key : 4
Admin Key : 0
Eth 1/1
------------------------------------------------------------------------
  LACPDUs Internal : 30 sec
  LACP System Priority : 32768
  LACP Port Priority : 32768
  Admin Key : 4
  Oper Key : 4
  Admin State : defaulted, aggregation, long timeout, LACP-activity
  Oper State : distributing, collecting, synchronization,
                aggregation, long timeout, LACP-activity
:
Console#
```

Displaying LACP Settings and Status for the Remote Side

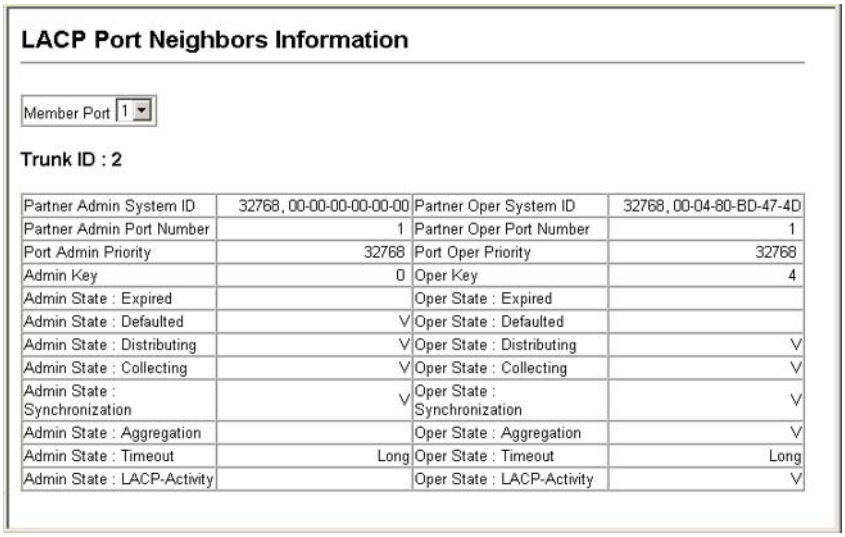
You can display configuration settings and the operational state for the remote side of an link aggregation.

Neighbor Configuration Information

Parameter	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

© 2004 Foundry Networks, Inc.

Web – Click Port, LACP, Port Neighbors Information. Select a port channel to display the corresponding information.



LACP Port Neighbors Information

Member Port 1

Trunk ID : 2

Partner Admin System ID	32768, 00-00-00-00-00-00	Partner Oper System ID	32768, 00-04-80-BD-47-4D
Partner Admin Port Number	1	Partner Oper Port Number	1
Port Admin Priority	32768	Port Oper Priority	32768
Admin Key	0	Oper Key	4
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted	V	Oper State : Defaulted	
Admin State : Distributing	V	Oper State : Distributing	V
Admin State : Collecting	V	Oper State : Collecting	V
Admin State : Synchronization	V	Oper State : Synchronization	V
Admin State : Aggregation		Oper State : Aggregation	V
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity		Oper State : LACP-Activity	V

CLI – The following example displays the LACP configuration settings and operational state for the remote side of port channel 1.

```
Console#show 1 lacp neighbors                                    4-182
Channel group 1 neighbors
-------------------------------------------------------------------------
Eth 1/1
-------------------------------------------------------------------------
  Partner Admin System ID : 32768, 00-00-00-00-00-00
  Partner Oper System ID : 32768, 00-00-00-00-00-01
  Partner Admin Port Number : 1
  Partner Oper Port Number : 1
  Port Admin Priority : 32768
  Port Oper Priority : 32768
  Admin Key : 0
  Oper Key : 4
  Admin State : defaulted, distributing, collecting, synchronization,
                long timeout,
  Oper State : distributing, collecting, synchronization,
               aggregation, long timeout, LACP-activity
⋮
Console#
```

Setting Broadcast Storm Thresholds

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

 © 2004 Foundry Networks, Inc.

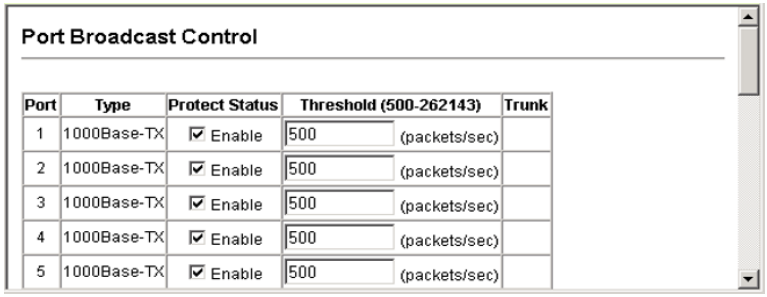
Command Usage

- Broadcast Control is enabled by default.
- The default threshold is:
  EdgeIron 4802CF, 2402CF, 24G-A, 48G - 500 packets per second
  EdgeIron 24G - 256 packets per second
- Broadcast Control does not affect IP multicast traffic.
- EdgeIron 4802CF, 2402CF, and 24G: The specified threshold applies to all ports on the switch.
- EdgeIron 24G-A and 48G: The specified threshold is set on a per port basis.

Command Attributes

- **Port** – Specifies a port.
- **Type** – Indicates the port type.
- **Protect Status** – Shows whether or not broadcast storm control has been enabled. (Default: Enabled)
- **Threshold** – Threshold as percentage of port bandwidth.
  - EdgeIron 4802CF, 2402CF, 24G-A and 48G – Range: 500-262143 packets per second; Default: 500 packets per second
  - EdgeIron 24G – Range: 16, 64, 128, or 256 packets per second; Default: 256 packets per second
- **Trunk** – Indicates if the port is a member of a trunk.

Web – Click Port, Port Broadcast Control. Set the threshold for all ports, and then click Apply.



CLI – Specify the required interface, and then enter the threshold. The following sets broadcast suppression at 600 packets per second on port 1.

```
Console(config)#interface ethernet 1/1                    4-109
Console(config-if)#switchport broadcast packet-rate 600   4-114
Console(config-if)#
```


© 2004 Foundry Networks, Inc.

Configuring Port Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

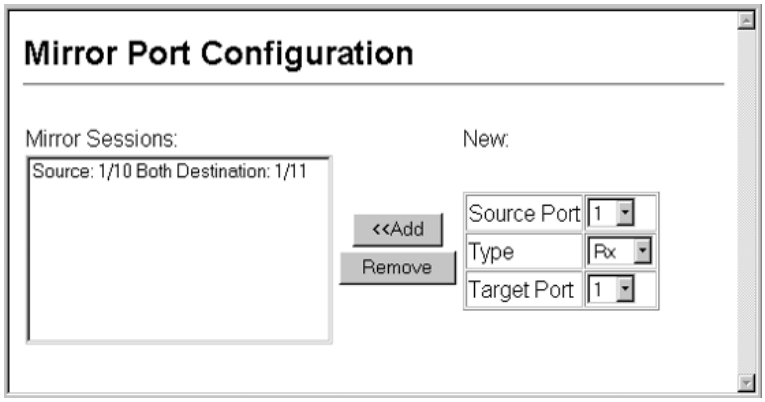
Command Usage

- The source port and target port speeds must match, otherwise traffic may be dropped from the source port.
- The EdgeIron 2402CF and 4802CF have this restriction:
  - All mirror sessions have to share the same target port.
- The EdgeIron 24G-A, 24G and 48G have these restrictions:
  - The switch supports only one port mirror session.
  - The source and target port have to be either both in the port group of 1 to 12 or both in the port group of 13 to 24; or in the case of the 48G - group 25 to 36 and group 37 to 48 as well.

Command Attributes

- **Mirror Sessions** – Displays a list of current mirror sessions.
- **Source Port** – The port whose traffic will be monitored.
- **Type** – Allows you to select the type of traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both.
- **Target Port** – The port that will “duplicate” or “mirror” the traffic on the source port.

Web – Click Port, Mirror. Specify the source port, the traffic type to be mirrored, and the target port, then click Add.



CLI – Use the interface command to select the target port, then use the port monitor command to specify the source port. Note that default mirroring under the CLI is for both received and transmitted packets.

```
Console(config)#interface ethernet 1/10                    4-109
Console(config-if)#port monitor ethernet 1/11              4-175
Console(config-if)#
```

 © 2004 Foundry Networks, Inc.

Configuring Rate Limits

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Command Usage

- The rate-limit range is:
  - Fast Ethernet interface – 1 to 100 Mbps
  - Gigabit Ethernet interface – 8 to 1000 Mbps
- The rate-limit resolution – The increment of change:
  - Fast Ethernet interface – 1 Mbps
  - Gigabit Ethernet interface – 8 Mbps

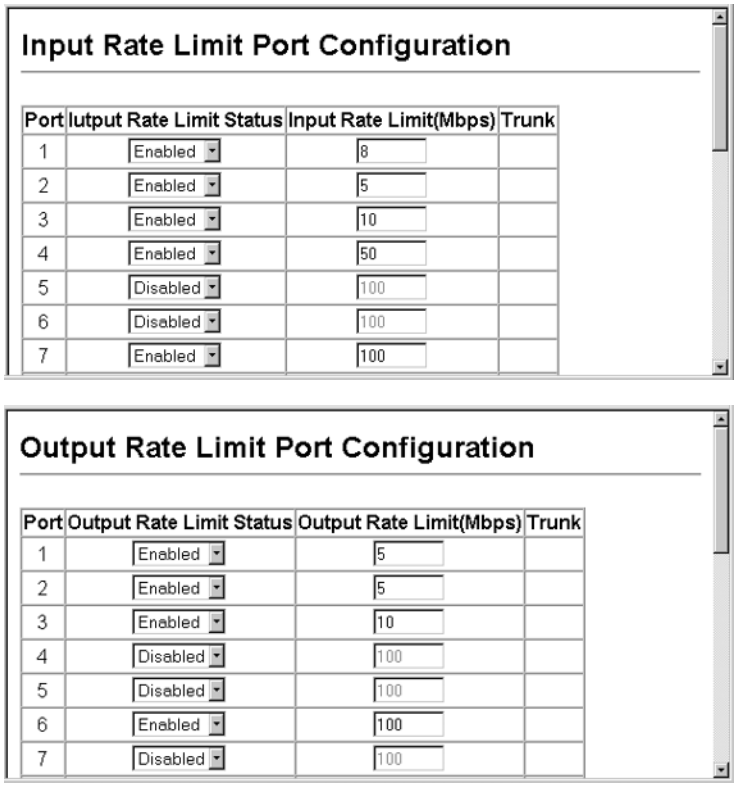
Note: The egress rate limit for the Gigabit uplink ports cannot be changed from the enable state to the disable state.

Command Attribute

- **Rate Limit** – Sets the input or output rate limit for an interface.
  - Default Status – Disabled
  - Default Rate – Fast Ethernet: 100 Mbps,
    Gigabit Ethernet: 1000 Mbps

© 2004 Foundry Networks, Inc.

Web – Click Rate Limit, Input/Output Rate Limit Port/Trunk Configuration. Set the Input/Output Rate Limit Status for selected interfaces, then set the rate limit and click Apply.



Input Rate Limit Port Configuration

Port	Iutput Rate Limit Status	Input Rate Limit(Mbps)	Trunk
1	Enabled	8	
2	Enabled	5	
3	Enabled	10	
4	Enabled	50	
5	Disabled	100	
6	Disabled	100	
7	Enabled	100	

Output Rate Limit Port Configuration

Port	Output Rate Limit Status	Output Rate Limit(Mbps)	Trunk
1	Enabled	5	
2	Enabled	5	
3	Enabled	10	
4	Disabled	100	
5	Disabled	100	
6	Enabled	100	
7	Disabled	100	

CLI - This example sets the rate limit for input and output traffic passing through port 1 to 60 Mbps.

```
Console(config)#interface ethernet 1/1                          4-109
Console(config-if)#rate-limit input 60                          4-186
Console(config-if)#rate-limit output 60                         4-186
Console(config-if)#
```

 © 2004 Foundry Networks, Inc.

Address Table Settings

Switches store the addresses for all known devices. This information is used to route traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

Setting Static Addresses

A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

Command Usage

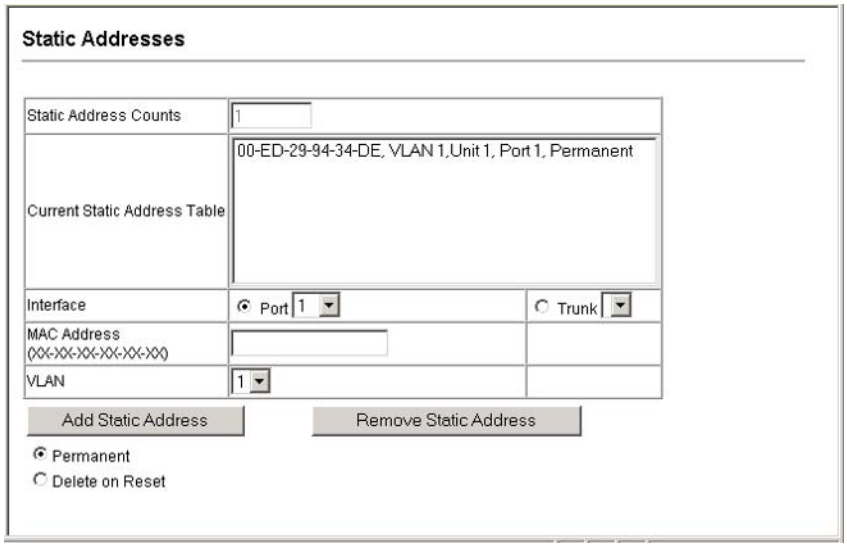
Entries specified via both the Web interface and the CLI can be made permanent or can be set to be deleted on reset.

Command Attributes

- **Static Address Counts*** – The number of manually configured addresses.
- **Current Static Address Table** – Lists all the static addresses.
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface.
- **VLAN** – ID of configured VLAN (1-4094).

*Web Only

Web – Click Address Table, Static Addresses. Specify the interface, the MAC address and VLAN, then click Add Static Address.



© 2004 Foundry Networks, Inc.

CLI – This example adds an address to the static address table, but sets it to be deleted when the switch is reset.

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface
  ethernet 1/1 vlan 1 delete-on-reset                        4-121
Console(config)#
```

Displaying the Address Table

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address is forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

Command Usage

- You can display entries in the dynamic address table by selecting an interface (either port or trunk), MAC address, or VLAN.
- You can sort the information displayed based on interface (port or trunk), MAC address, or VLAN.

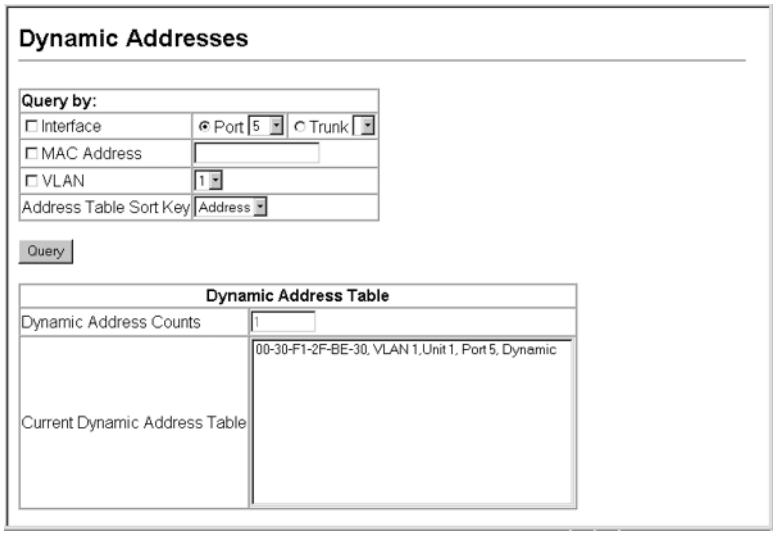
Command Attributes

- **Interface** – Indicates a port or trunk.
- **MAC Address** – Physical address associated with this interface.
- **VLAN** – ID of configured VLAN (1-4094).
- **Address Table Sort Key** – You can sort the information displayed based on interface (port or trunk) or MAC address.
- **Dynamic Address Counts** – The number of addresses dynamically learned.
- **Current Dynamic Address Table** – Lists all the dynamic addresses.

 © 2004 Foundry Networks, Inc.

Web – Click Address Table, Dynamic Addresses. Specify the search type (i.e., Interface, MAC Address, or VLAN), the method of sorting the displayed addresses, then click Query.

For example, the following screen shows the dynamic addresses for port 5.



CLI – This example displays the address table entries for port 11.

```
Console#show mac-address-table interface ethernet 1/11      4-122
 Interface Mac Address         Vlan  Type
 --------- -----------------   ----  -----------------
  Eth 1/11 00-10-b5-62-03-74    1    Learned
Console#
```

Changing the Aging Time

You can set the aging time for entries in the dynamic address table.

Command Usage

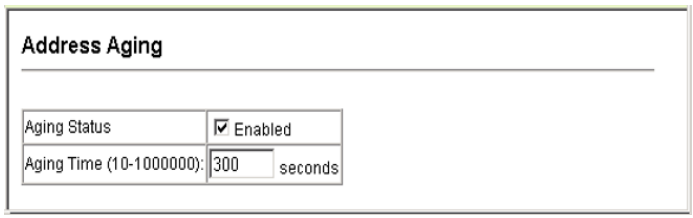
- EdgeIron 4802CF, 2402CF, 48G and 24G-A: The range for the aging time is 10 - 1000000 seconds. (The default is 300 seconds.)
- EdgeIron 24G: The range for the aging time is 17 - 2184 seconds. (The default is 300 seconds.)

Command Attributes

- **Aging Status** – Enables or disables the aging time.
- **Aging Time** – The time after which a learned entry is discarded. (Range: 10-1000000 seconds; Default: 300 seconds)

© 2004 Foundry Networks, Inc.

Web – Click Address Table, Address Aging. Check "Aging Status", specify the new aging time, then click Apply.



CLI – This example sets the aging time to 400 seconds.

```
Console(config)#mac-address-table aging-time 400            4-123
Console(config)#
```

Spanning Tree Protocol

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (i.e., an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links that automatically take over when a primary link goes down.

The Spanning Tree Protocols supported by the switch include the following standards:

- **STP** – Spanning Tree Protocol (IEEE 802.1D).
- **RSTP** – Rapid Spanning Tree Protocol (IEEE 802.1w).
- **Per VLAN STP** – Foundry Per VLAN spanning tree backward compatible

STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) that incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN that incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

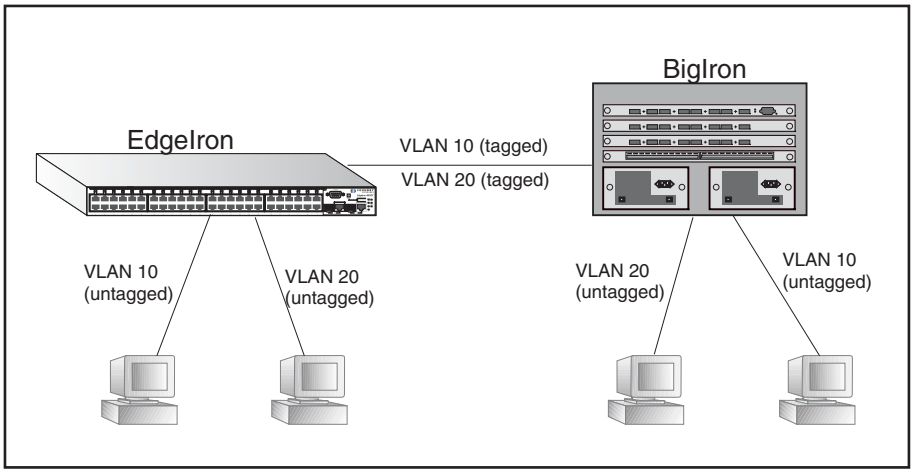
 © 2004 Foundry Networks, Inc.

RSTP is designed as a general replacement for the slower, legacy STP. RSTP achieves much faster reconfiguration (around one tenth of that required by STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

Enabling a Single Instance of STP per VLAN on an EdgeIron

When you create a port-based VLAN on a Foundry Layer 2 Switch, a Spanning Tree Protocol (STP) instance is automatically created for the VLAN. In addition, the default VLAN has its own instance of STP. (Refer to the "Configuring Spanning Tree Protocol" chapter in the *Foundry Switch and Router Installation and Basic Configuration Guide*.)

A VLAN with its own STP instance ensures that it is isolated from STP problems that may occur in other VLANs. The following figure shows VLANs 10 and 20 configured on an EdgeIron and a BigIron. Any STP activity caused by network problems that occur in VLAN 10 will never be propogated in VLAN 20.



© 2004 Foundry Networks, Inc.

To display VLAN settings and configure a VLAN with an STP instance on the EdgeIron 24G-A, enter the following commands:

```
Console#show  vlan
VLAN Type    Name     Status    Ports/Channel groups
---- ------- ---------------- --------- ---------------------------------------
   1  Static                   Active   Eth1/ 1 Eth1/ 4 Eth1/ 5 Eth1/ 6 Eth1/ 7
                                                Eth1/ 8 Eth1/ 9 Eth1/10 Eth1/11 Eth1/12
                                                Eth1/13 Eth1/14 Eth1/15 Eth1/16 Eth1/17
                                                Eth1/18 Eth1/19 Eth1/20 Eth1/21 Eth1/22
                                                 Eth1/23 Eth1/24 Eth1/25 Eth1/26
   2  Static                     Active
Console#configure terminal
Console(config)#vlan 10
Console(config-vlan-10)#tagged ethernet 1/2
Console(config-vlan-10)#tagged ethernet 1/3
Console(config-vlan-10)#untag ethernet to 1/4
Console(config-vlan-10)#exit
Console(config)#vlan 20
Console(config-vlan-10)#tagged ethernet 1/2
Console(config-vlan-10)#tagged ethernet 1/3
Console(config-vlan-20)#untag ethernet 1/5
Console(config-if)#exit
Console(config)#spanning-tree mst configuration
Console(config-mstp)#mst 10 priority 40960
Console(config-mstp)#mst 20 priority 4096
Console(config-mstp)#exit
Console(config)#exit
```

The example above allows EdgeIron to have a distinct STP for VLAN 10 and one for VLAN 20.

Note: Make sure that only one VLAN is assigned to an STP instance on the EdgeIron, otherwise, it will not work.

On the BigIron Layer 2 Switch, create VLANs with the same VLAN IDs as those on the EdgeIron device as follows.

```
BigIron(config)#vlan 10
BigIron(config-vlan-10)#tagged ethernet 2/10
BigIron(config-vlan-10)#untag ethernet 3/5
BigIron(config-vlan-10)#exit
BigIron(config)#vlan 20
BigIron(config-vlan-20)#tagged ethernet 2/10
BigIron(config-vlan-20)#untagged ethernet 3/8
BigIron(config-vlan-20)#exit
BigIron(config)#
```

STP Information

The Spanning Tree, STP Information page contains information on the current status of the spanning tree.

Command Attributes

- **Spanning Tree State** – Indicates if the Spanning Tree Protocol is currently enabled on the switch.
- **Bridge ID** – Identifies a unique identifier for the switch in the spanning tree. The ID is calculated using the defined spanning tree priority of the switch and its MAC address. The lower the Bridge ID, the more likely the switch will act as the root.
- **Max Age** – The maximum time (in seconds) the switch can wait without receiving a configuration

 © 2004 Foundry Networks, Inc.

message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. If the root port ages out STP information (provided in the last configuration message), a new root port is selected from among the device ports attached to the network. (References to “ports” in this section means “interfaces,” which includes both ports and trunks.)

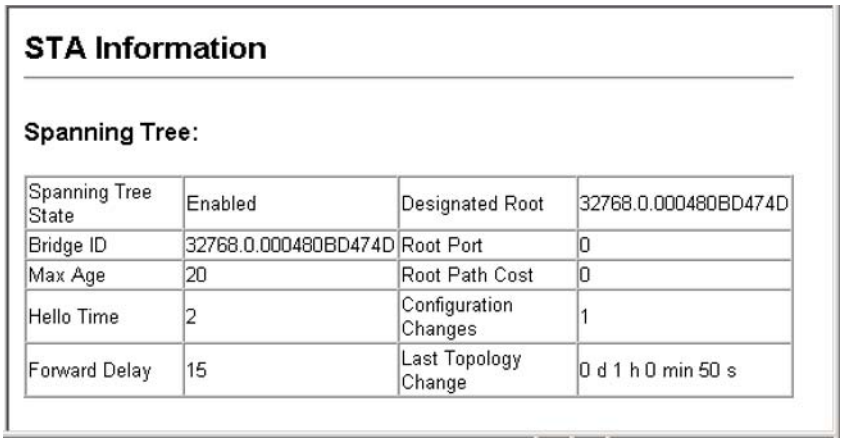
- **Hello Time** – Specifies the time interval (in seconds) at which the root device transmits a configuration message.
- **Forward Delay** – The maximum time (in seconds) the switch will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Designated Root** – Identifies the priority and MAC address of the device in the spanning tree that the switch has accepted as the root device.
- **Root Port** – Specifies the port number on the switch that is closest to the root. The switch communicates with the root device through this port. If there is no root port, the switch has been accepted as the root device of the spanning tree network.
- **Root Path Cost** – Identifies the path cost from the root port on the switch to the root device.
- **Root Hello Time*** – Interval (in seconds) at which this device transmits a configuration message.
- **Root Maximum Age*** – The maximum time (in seconds) this device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. If the root port ages out STP information (provided in the last configuration message), a new root port is selected from among the device ports attached to the network.(References to “ports” in this section means “interfaces,” which includes both ports and trunks.)
- **Root Forward Delay*** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Configuration Changes** – Specifies the number of times the spanning tree has been reconfigured.
- **Last Topology Change** – Identifies the time since the spanning tree was last reconfigured.

* CLI Only

Note: The term STP has been substituted by the term STA in the web screen interface.

 © 2004 Foundry Networks, Inc.

Web – Click Spanning Tree, STP Information to display current spanning tree information.



STA Information

Spanning Tree:

Spanning Tree State	Enabled	Designated Root	32768.0.000480BD474D
Bridge ID	32768.0.000480BD474D	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	1
Forward Delay	15	Last Topology Change	0 d 1 h 0 min 50 s

CLI – This example shows the current spanning tree settings.

```
Console#show spanning-tree                                        4-137
Spanning-tree information
----------------------------------------------------------------------
 Spanning tree mode               :RSTP
 Spanning tree enable/disable     :enable
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Designated Root                  :32768.000011112222
 Current root port                :0
 Current root cost                :0
 Number of topology changes       :1
 Last topology changes time (sec.):10811
 Transmission limit               :3
 Path Cost Method                 :long
----------------------------------------------------------------------
Eth  1/ 1 information
----------------------------------------------------------------------
 Admin status         : enable
 Role                 : disable
 State                : discarding
 Path cost            : 10000
 Priority             : 128
 Designated cost      : 0
 Designated port      : 128.1
 Designated root      : 32768.000011112222
 Designated bridge    : 32768.000011112222
 Fast forwarding      : disable
 Forward transitions  : 0
 Admin edge port      : disable
 Oper edge port       : disable
 Admin Link type      : auto
 Oper Link type       : point-to-point

Eth  1/ 2 information
----------------------------------------------------------------------
 Admin status         : enable
 Role                 : disable
 State                : discarding
 Path cost            : 10000
.
.
Console#
```

 © 2004 Foundry Networks, Inc.

STP Configuration

Global settings apply to the entire switch.

Command Usage

The Rapid Spanning Tree Protocol (RSTP) supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

- **STP Mode** – If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
- **RSTP Mode** – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

© 2004 Foundry Networks, Inc.

Note: The **spanning-tree mode** command has been removed and replaced by RSTP mode for the global spanning tree and PVST-compliant mode for each VLAN. If the switch detects a device running STP it will automatically downgrade to STP. Presently the firmware does not support MSTP.

Command Attributes

- **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority and MAC address (where the address is taken from the switch system).
- **Spanning Tree State** – Enables or disables the spanning tree. If you enable the spanning tree, you must complete the other fields.
  (Default: enabled)
- **Spanning Tree Type** – Specifies the type of Spanning Tree Protocol used on the switch:
  (Default: RSTP)
  - **STP**: (IEEE 802.1D; i.e., when this option is selected, the switch will use RSTP set to STP forced-compatibility mode). When operating multiple VLANs, we recommend selecting the MSTP option.
  - **RSTP**: Rapid Spanning Tree Protocol (IEEE 802.1w)

Note: A Spanning Tree instance can exist only on bridges that have compatible VLAN instance assignments.

Note: Be careful when switching between Spanning Tree modes. Changing modes stops all Spanning Tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
  - Default: 32768
  - Range: 0-61440, in steps of 4096
  - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440
- **Hello Time** – Interval (in seconds) at which the switch transmits a configuration message.
  - Default: 2
  - Minimum: 1
  - Maximum: The lower of 10 or [(Max. Message Age / 2) -1]

 © 2004 Foundry Networks, Inc.

- **Maximum Age** – The maximum time (in seconds) the switch can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section means "interfaces," which includes both ports and trunks.)

  - Default: 20
  - Minimum: The higher of 6 or [2 x (Hello Time + 1)].
  - Maximum: The lower of 40 or [2 x (Forward Delay - 1)]
- **Forward Delay** – The maximum time (in seconds) the switch will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

  - Default: 15
  - Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
  - Maximum: 30
- **Max Instance Numbers** — The maximum number of MSTP instances to which the switch can be assigned. (Default: 65)

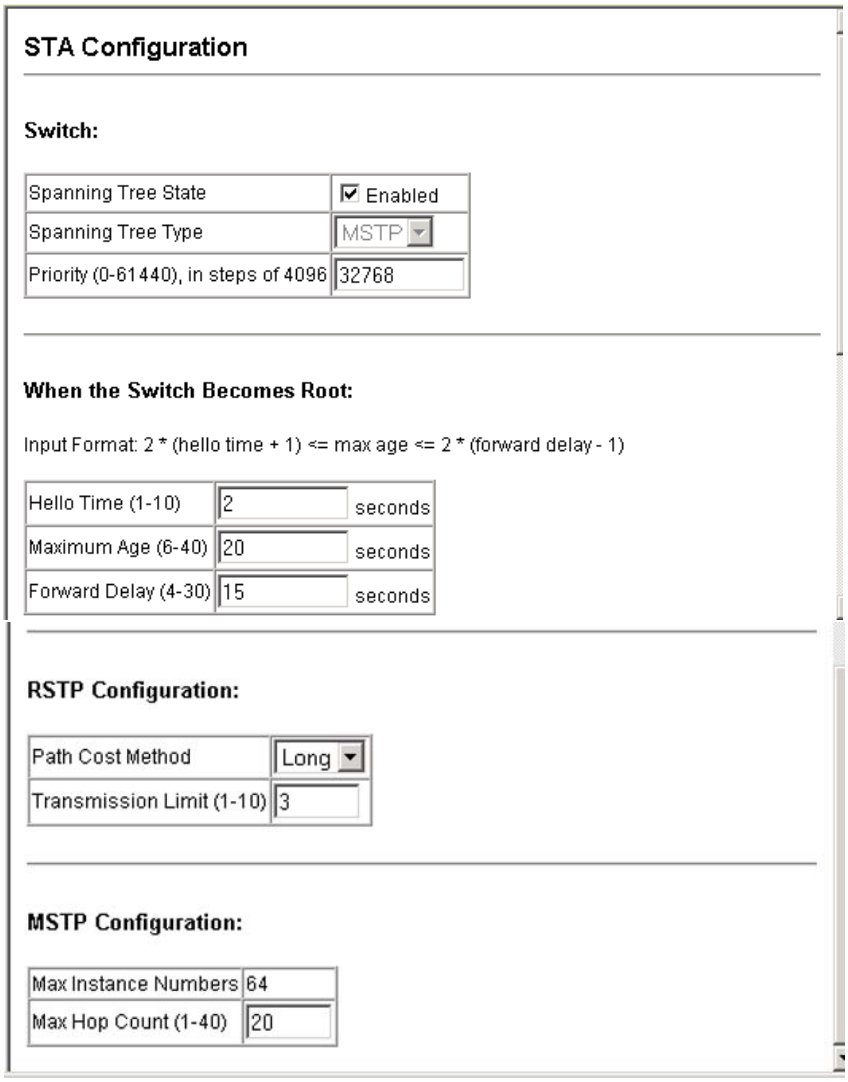
- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

  - **Long**: Specifies 32-bit based values that range from 1-200,000,000.
  - **Short**: Specifies 16-bit based values that range from 1-65535. (This is the default.)
- **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

- **Max Hop Counts** — The maximum number of hops allowed in this MSTI region before a BPDU is discarded. (Range: 1-40; Default: 20)

© 2004 Foundry Networks, Inc.

Web – Click Spanning Tree, STP Configuration. Modify the required attributes, then click Apply.



CLI – This example enables Spanning Tree Protocol, and then sets the indicated attributes.

```
Console(config)#spanning-tree mode rstp                    4-125
Console(config)#spanning-tree                              4-125
Console(config)#spanning-tree forward-time 15              4-126
Console(config)#spanning-tree hello-time 2                 4-126
Console(config)#spanning-tree max-age 20                   4-127
Console(config)#spanning-tree priority 40000               4-127
Console(config)#spanning-tree pathcost method long         4-128
Console(config)#spanning-tree transmission-limit 5         4-128
Console(config)#spanning-tree mst-configuration            4-129
Console(config-mstp)#name r&d                              4-131
Console(config-mstp)#revision 1                            4-132
Console(config-mstp)#max-hops 30                           4-132
Console(config-mstp)#
```

 © 2004 Foundry Networks, Inc.

STP Port and Trunk Information

The Spanning Tree/STP Port Information and STP Trunk Information display the current status of ports and trunks in the spanning tree.

Command Attributes

- **STP Status** – Displays current state of this port within the spanning tree:
  - **Discarding** – Port receives STP configuration messages, but does not forward packets.
  - **Learning** – Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** – Port forwards packets, and continues learning addresses.

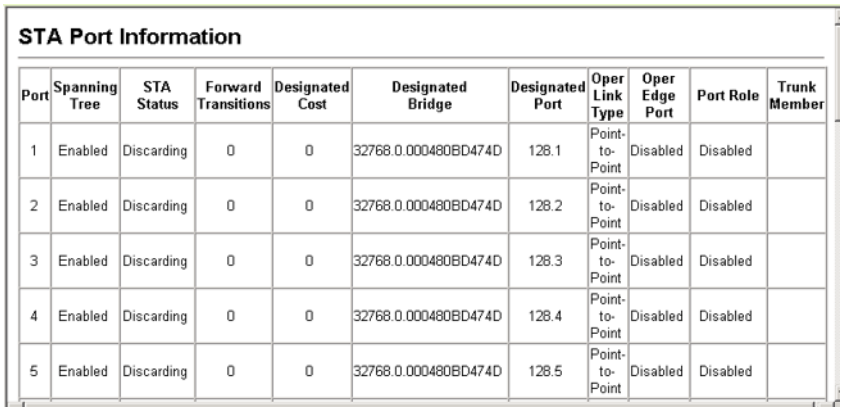
  The rules defining port status are:
  - A port on a network segment with no other STP-compliant bridging device is always forwarding.
  - If two ports on a switch are connected to the same segment and there is no other STP device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
  - All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.
- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.
- **Designated Cost** – The cost for a packet to travel from this port to the root in the current spanning tree configuration. The slower the media, the higher the cost.
- **Designated Bridge** – The priority and MAC address of the device through which this port must communicate to reach the root of the spanning tree.
- **Designated Port** – The priority and number of the port on the designated bridging device through which this switch must communicate with the root of the spanning tree.
- **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for “Admin Link Type” in the STP Port/Trunk Configuration page.
- **Oper Edge Port** – This parameter is initialized to the setting for “Admin Edge Port” in the STP Port/Trunk Configuration page (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
- **Port Role** – Roles are assigned according to whether the port is part of the active spanning tree topology:
  - **Root:** The port is connecting the bridge to the root bridge.
  - **Designated:** The port is connecting a LAN through the bridge to the root bridge.
  - **Alternate** or **Backup:** A port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed.
  - **Disabled:** The role is set to disabled if a port has no role within the spanning tree.
- **Trunk Member** – Indicates whether the port is configured as a trunk member. (STP Port Information page only.)

 © 2004 Foundry Networks, Inc.

These additional parameters are only displayed in the CLI:

- **Admin status** – Shows if STP has been enabled on this interface.
- **Path Cost** – This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)
- **Priority** – Defines the priority used for this port in the spanning tree. If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the spanning tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with the lowest numeric identifier will be enabled.
- **Designated root** – The priority and MAC address of the device in the spanning tree that this switch has accepted as the root device.
- **Fast forwarding** – This field provides the same information as Admin Edge port, and is only included for backward compatibility with earlier products.
- **Admin Link Type** – The link type attached to this interface.
  - **Point-to-Point** – A connection to exactly one other bridge.
  - **Shared** – A connection to two or more bridges.
  - **Auto** – The switch automatically determines if the interface is attached to a point-to-point link or to shared media.
- **Admin Edge Port** – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to reconfigure when the interface changes state, and also overcomes other STP-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.

Web – Click Spanning Tree, STP Port Information or STP Trunk Information.



STA Port Information

Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Enabled	Discarding	0	0	32768.0.000480BD474D	128.1	Point-to-Point	Disabled	Disabled	
2	Enabled	Discarding	0	0	32768.0.000480BD474D	128.2	Point-to-Point	Disabled	Disabled	
3	Enabled	Discarding	0	0	32768.0.000480BD474D	128.3	Point-to-Point	Disabled	Disabled	
4	Enabled	Discarding	0	0	32768.0.000480BD474D	128.4	Point-to-Point	Disabled	Disabled	
5	Enabled	Discarding	0	0	32768.0.000480BD474D	128.5	Point-to-Point	Disabled	Disabled	

 © 2004 Foundry Networks, Inc.

CLI – This example displys the current spanning tree status of a port.

```
Console#show spanning-tree ethernet 1/5                    4-137
Eth  1/ 5 information
---------------------------------------------------------------
 Admin status         : enable
 Role                 : designate
 State                : forwarding
 Path cost            : 100000
 Priority             : 128
 Designated cost      : 0
 Designated port      : 128.5
 Designated root      : 32768.000011112222
 Designated bridge    : 32768.000011112222
 Fast forwarding      : disable
 Forward transitions  : 1
 Admin edge port      : disable
 Oper edge port       : disable
 Admin Link type      : auto
 Oper Link type       : point-to-point

Console#
```

STP Port and Trunk Configuration

You can configure RSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding. (References to “ports” in this section means “interfaces,” which includes both ports and trunks.)

Command Attributes

- **Port** — Specifies a port.
- **Spanning Tree**l — Check to enable spanning tree on a port.
- **STA State** – Displays current state of this port within the spanning tree:
  - **Discarding** – Port receives STP configuration messages, but does not forward packets.
  - **Learning** – Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** – Port forwards packets, and continues learning addresses.
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the spanning tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. (Default: 128; Range: 0-240, in steps of 16)

 © 2004 Foundry Networks, Inc.

- **Path Cost** – This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)

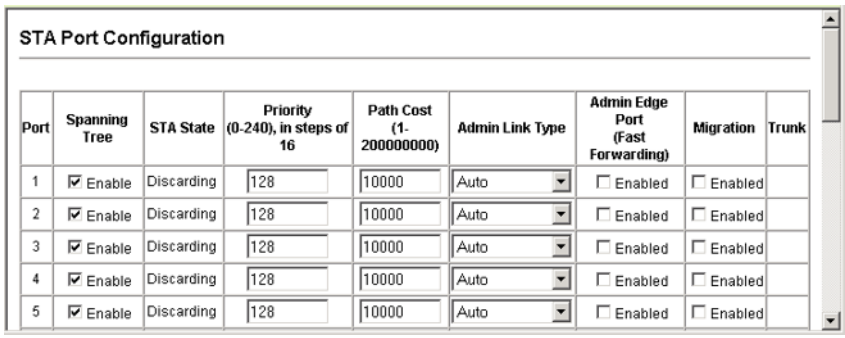
  - Range –
    Ethernet: 200,000-20,000,000
    Fast Ethernet: 20,000-2,000,000
    Gigabit Ethernet: 2,000-200,000
  - Defaults –
    Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
    Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000
    Gigabit Ethernet – full duplex: 10,000; trunk: 5,000

Note: When the Path Cost Method is set to short, the maximum path cost is 65,535.

- **Admin Link Type** – The link type attached to this interface. (Default: Auto)

  - **Point-to-Point** – A connection to exactly one other bridge.
  - **Shared** – A connection to two or more bridges.
  - **Auto** – The switch automatically determines if the interface is attached to a point-to-point link or to shared media.
- **Admin Edge Port** – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STP-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- **Migration** – Re-checks the appropriate BPDU format to send on the selected interface. If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also check this Migration check box to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces.
- **Trunk** – Specifies if a port is member of a trunk.

Web – Click Spanning Tree, STP Port Configuration or STP Trunk Configuration. Modify the required attributes, then click Apply.


STA Port Configuration
Port
Spanning Tree
STA State
Priority (0-240), in steps of 16
Path Cost (1-200000000)
Admin Link Type
Admin Edge Port (Fast Forwarding)
Migration
Trunk
1 Enable Discarding 128 10000 Auto Enabled Enabled
2 Enable Discarding 128 10000 Auto Enabled Enabled
3 Enable Discarding 128 10000 Auto Enabled Enabled
4 Enable Discarding 128 10000 Auto Enabled Enabled
5 Enable Discarding 128 10000 Auto Enabled Enabled

 © 2004 Foundry Networks, Inc.

CLI – This example sets STP attributes for port 5.

```
Console(config)#interface ethernet 1/5                          4-109
Console(config-if)#spanning-tree port-priority 128              4-134
Console(config-if)#spanning-tree cost 19                        4-133
Console(config-if)#spanning-tree link-type auto                 4-136
Console(config-if)#no spanning-tree edge-port                   4-135
Console#spanning-tree protocol-migration ethernet 1/5           4-136
Console#
```

Multiple Spanning Tree Protocol Configuration

Notes: 1. All settings for MSTP are applicable to PVST configuration.

2. The **spanning-tree mode** command has been removed and replaced by RSTP mode for the global spanning tree and PVST-compliant mode for each VLAN. If the switch detects a device running STP it will automatically downgrade to STP. Presently the firmware does not support MSTP.

MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

By default all VLANs are assigned to the Internal Spanning Tree (MST Instance 0) that connects all bridges and LANs within the MST region. This switch supports up to 65 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region (page 3-89) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

To use multiple spanning trees:

- Set the spanning tree type to MSTP (STP Configuration, page 3-77).
- Enter the spanning tree priority for the selected MST instance (MSTP VLAN Configuration).
- Add the VLANs that will share this MSTI (MSTP VLAN Configuration).

Note: All VLANs are automatically added to the IST (Instance 0).

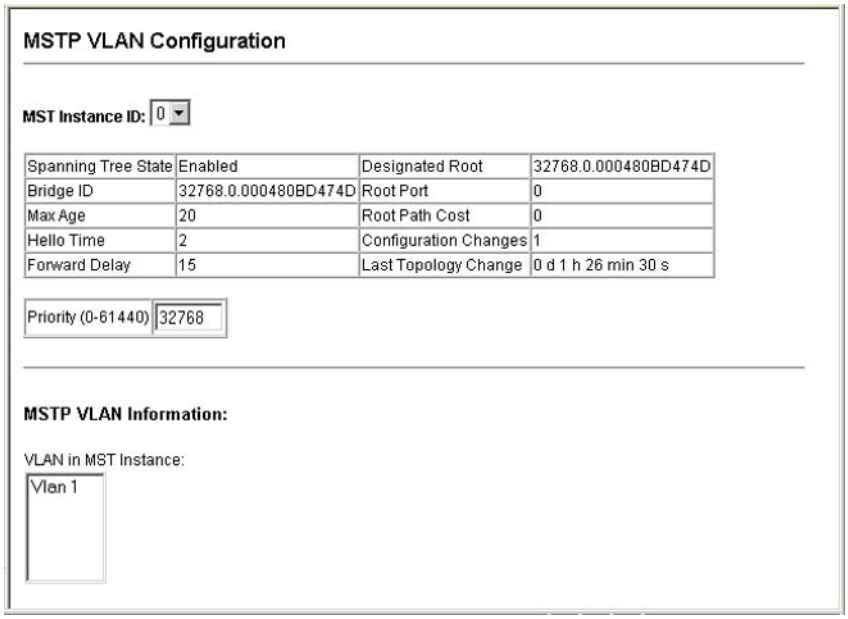
To ensure that the MSTI maintains connectivity across the network, you must configure a related set of bridges with the same MSTI settings.Command Attributes

- **MST Instance** – Instance identifier of this spanning tree. (Default: 0)
- **Priority** – The priority of a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440; Default: 32768)
- **VLANs in MST Instance** – VLANs assigned this instance.

 © 2004 Foundry Networks, Inc.

The other global attributes are described under “Displaying Interface Settings for MSTP,” page 33-87. The attributes displayed by the CLI for individual interfaces are described under “Spanning Tree Commands,” page 44-139.

Web – Click Spanning Tree, MSTP, VLAN Configuration. Select an instance identifier from the list, set the instance priority, and click Apply. To add the VLAN members to an MSTI instance, enter the instance identifier, the VLAN identifier, and click Add.


MSTP VLAN Configuration
MST Instance ID: 0
Spanning Tree State Enabled Designated Root 32768.0.000480BD474D
Bridge ID 32768.0.000480BD474D Root Port 0
Max Age 20 Root Path Cost 0
Hello Time 2 Configuration Changes 1
Forward Delay 15 Last Topology Change 0 d 1 h 26 min 30 s
Priority (0-61440) 32768
MSTP VLAN Information:
VLAN in MST Instance:
Vlan 1

 © 2004 Foundry Networks, Inc.

CLI – This displays STP settings for instance 1, followed by settings for each port.

```
Console#show spanning-tree mst 2                              4-138
Spanning-tree information
----------------------------------------------------------------
 Spanning tree mode               :MSTP
 Spanning tree enable/disable     :enable
 Instance                         :2
 Vlans configuration              :2
 Priority                         :4096
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Max hops                         :20

 Remaining hops                   :20
 Designated Root                  :4096.2.0000E9313131
 Current root port                :0
 Current root cost                :0
 Number of topology changes       :0
 Last topology changes time (sec.):646
 Transmission limit               :3
 Path Cost Method                 :long
----------------------------------------------------------------
Eth  1/ 7 information
----------------------------------------------------------------
 Admin status         : enable
 Role                 : disable
 State                : discarding
 External path cost   : 10000
 Internal path cost   : 10000
 Priority             : 128
 Designated cost      : 0
 Designated port      : 128.7
 Designated root      : 4096.2.0000E9313131
 Designated bridge    : 4096.2.0000E9313131
 Fast forwarding      : enable
 Forward transitions  : 0
 Admin edge port      : enable
 Oper edge port       : enable
 Admin Link type      : auto
 Oper Link type       : point-to-point
 Spanning Tree Status : enable
.
.
```

CLI – This example sets the priority for MSTI 1, and adds VLANs 1-5 to this MSTI.

```
Console(config)#spanning-tree mst-configuration          4-139
Console(config-mst)#mst 1 priority 4096                  4-131
Console(config-mstp)#mst 1 vlan 1-5                      4-130
Console(config-mst)#
```

Displaying Interface Settings for MSTP

The MSTP Port Information and MSTP Trunk Information pages display the current status of ports and trunks in the selected MST instance.

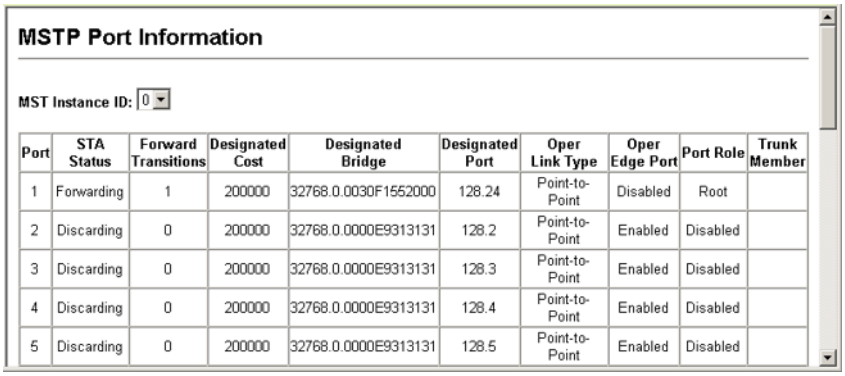
Field Attributes:

- **MST Instance ID** – Instance identifier to configure. (Range: 0-57; Default: 0)

The other attributes are described under “Configuring Interface Settings for MSTP,” page 33-89.

 © 2004 Foundry Networks, Inc.

Web – Click Spanning Tree, MSTP Port Information or MSTP Trunk Information. Select the required MST instance to display the current spanning tree values.



MSTP Port Information

MST Instance ID: 0

Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Forwarding	1	200000	32768.0.0030F1552000	128.24	Point-to-Point	Disabled	Root	
2	Discarding	0	200000	32768.0.0000E9313131	128.2	Point-to-Point	Enabled	Disabled	
3	Discarding	0	200000	32768.0.0000E9313131	128.3	Point-to-Point	Enabled	Disabled	
4	Discarding	0	200000	32768.0.0000E9313131	128.4	Point-to-Point	Enabled	Disabled	
5	Discarding	0	200000	32768.0.0000E9313131	128.5	Point-to-Point	Enabled	Disabled	

CLI – This displays STP settings for instance 0, followed by settings for each port. The settings for instance 0 are global settings that apply to the IST (page 33-77), the settings for other instances only apply to the local spanning tree.

```
Console#show spanning-tree mst 0                              4-139
Spanning-tree information
----------------------------------------------------------------------
 Spanning tree mode               :MSTP
 Spanning tree enable/disable     :enable
 Instance                         :0
 Vlans configuration              :1-4094
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Max hops                         :20
 Remaining hops                   :20
 Designated Root                  :32768.0.0000ABCD0000
 Current root port                :1
 Current root cost                :200000
 Number of topology changes       :1
 Last topology changes time (sec.):645
 Transmission limit               :3
 Path Cost Method                 :long
----------------------------------------------------------------------
Eth  1/ 1 information
----------------------------------------------------------------------
 Admin status         : enable
 Role                 : root
 State                : forwarding
 External path cost   : 100000
 Internal path cost   : 100000
 Priority             : 128
 Designated cost      : 200000
 Designated port      : 128.24
 Designated root      : 32768.0.0000ABCD0000
 Designated bridge    : 32768.0.0030F1552000
 Fast forwarding      : disable
 Forward transitions  : 1
 Admin edge port      : enable
 Oper edge port       : disable
 Admin Link type      : auto
 Oper Link type       : point-to-point
 Spanning Tree Status : enable
.
.
.
```

 © 2004 Foundry Networks, Inc.

Configuring Interface Settings for MSTP

You can configure the STP interface settings for an MST Instance using the MSTP Port Configuration and MSTP Trunk Configuration pages.

Field Attributes:

The following attributes are read-only and cannot be changed:

- **STA State** – Displays current state of this port within the Spanning Tree. (See STP Port and Trunk Information on page 33-81 for additional information.)
  - **Discarding** - Port receives STP configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.
- **Trunk** – Indicates if a port is a member of a trunk. (STP Port Configuration only)

The following interface attributes can be configured:

- **MST Instance ID** – Instance identifier to configure. (Range: 0-57; Default: 0)
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
  - Default: 128
  - Range: 0-240, in steps of 16
- **MST Path Cost** – This parameter is used by the MSTP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 3-63), the maximum path cost is 65,535.
  - Range –
    - Ethernet: 200,000-20,000,000
    - Fast Ethernet: 20,000-2,000,000
    - Gigabit Ethernet: 2,000-200,000
  - Default –
    - Ethernet – Half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
    - Fast Ethernet – Half duplex: 200,000; full duplex: 100,000; trunk: 50,000
    - Gigabit Ethernet – Full duplex: 10,000; trunk: 5,000

© 2004 Foundry Networks, Inc.

VLAN Configuration

In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle traffic such as IPX or NetBEUI. By using IEEE 802.1Q-compliant VLANs, you can organize any group of network nodes into separate broadcast domains, thus confining broadcast traffic to the originating group. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the PVID of the receiving port. But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

 © 2004 Foundry Networks, Inc.

Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by using a Layer-3 router or switch.

Untagged VLANs – Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets. However, you should use IEEE 802.3 tagged VLANs with GVRP whenever possible to fully automate VLAN registration.

Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system whereby the switch can automatically learn the VLANs to which each endstation should be assigned. If an endstation (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

To implement GVRP in a network, first add the host devices to the required VLANs (using the operating system or other application software), so that these VLANs can be propagated onto the network. For both the edge switches attached directly to these hosts, and core switches in the network, enable GVRP on the links between these devices. You should also determine security boundaries in the network and disable GVRP on ports to prevent advertisements being propagated, or forbid ports from joining restricted VLANs.

If you have host devices that do not support GVRP, you must configure static VLANs for the switch ports connected to these devices. You also still need to enable GVRP on these edge switches, as well as on the core switches in the network.

Forwarding Tagged/Untagged Frames

If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you need to create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from the switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from the switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when the switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

 © 2004 Foundry Networks, Inc.

Enabling or Disabling GVRP (Global Setting)

GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch. (Default: Disabled)

Web – Click VLAN, 802.1Q VLAN, GVRP Status. Enable or disable GVRP, and click Apply.



CLI – This example enables GVRP for the switch.

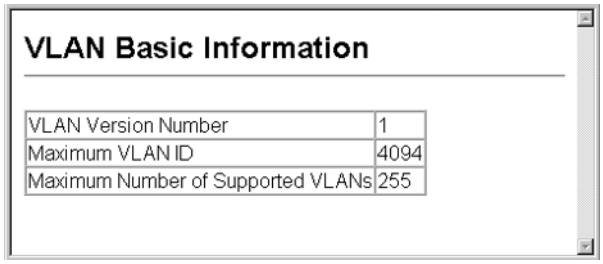
```
Console(config)#bridge-ext gvrp                                    4-156
Console(config)#
```

Displaying Basic VLAN Information

Command Attributes

- **VLAN Version Number** – The VLAN version used by this switch as specified in the IEEE 802.1Q standard. (Web interface only.)
- **Maximum VLAN ID** – Maximum VLAN ID recognized by this switch.
- **Maximum Number of Supported VLANs** – Maximum number of VLANs that can be configured on this switch.

Web – Click VLAN, 802.1Q VLAN, Basic Information.



© 2004 Foundry Networks, Inc.

CLI – Enter the following command.

```
Console#show bridge-ext                                          4-157
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Enabled
 GMRP: Disabled
Console#
```

Displaying Current VLANs

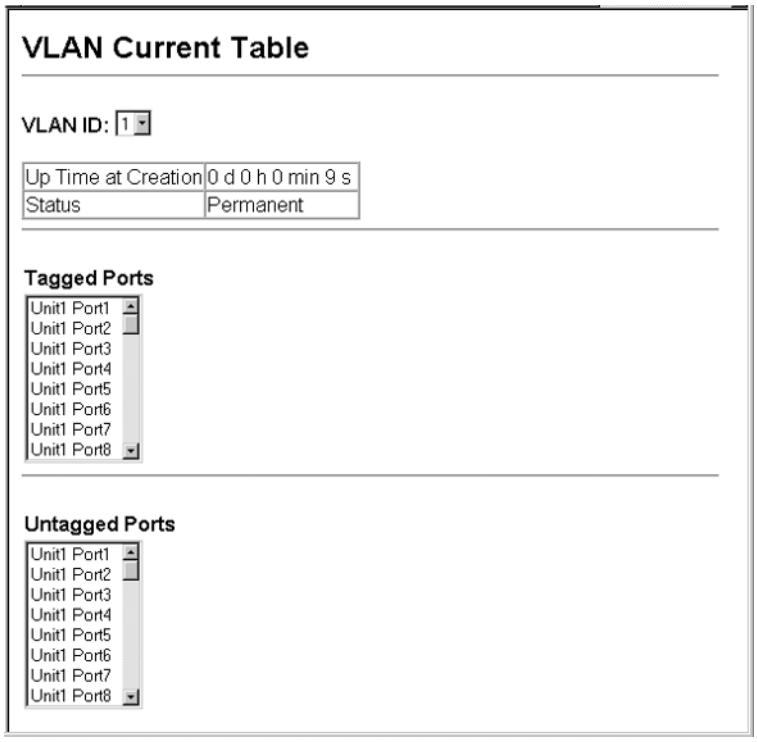
The VLAN Current Table shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can disable tagging.

Command Attributes for Web Interface

- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).
- **Up Time at Creation** – Time this VLAN was created; i.e., System Up Time.
- **Status** – Shows how this VLAN was added to the switch.
  - **Dynamic GVRP**: Automatically learned via GVRP.
  - **Permanent**: Added as a static entry.
- **Tagged Ports** – Shows the tagged VLAN port members.
- **Untagged Ports** – Shows the untagged VLAN port members

© 2004 Foundry Networks, Inc.

Web – Click VLAN, 802.1Q VLAN, Current Table. Select any ID from the scroll-down list.



Command Attributes for CLI Interface

- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes).
- **Type** – Shows how this VLAN was added to the switch.
  - **Dynamic**: Automatically learned via GVRP.
  - **Static**: Added as a static entry.
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Shows if this VLAN is enabled or disabled.
  - **Active**: VLAN is operational.
  - **Suspend**: VLAN is suspended; i.e., does not pass packets.
- **Ports / Channel groups** – Shows the VLAN interface members.

Note: The maximum length of a VLAN name is 32 characters (the same as RFC2674 MIB definition). When a VLAN name is set through the ifAlias object (RFC2863 MIB), up to 64 characters can be used, but the name is always truncated to 32 characters, because both refer to the same database. The maximum lengths for all other names (such as ports and trunks) are 64 characters.

© 2004 Foundry Networks, Inc.

CLI – Current VLAN information can be displayed with the following command.

```
Console#show vlan id 1                                                    4-148
VLAN Type    Name             Status    Ports/Channel groups
---- ------- ---------------- --------- -------------------------------------
   1  Static      DefaultVlan    Active Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4 Eth1/ 5
                                        Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9 Eth1/10
                                        Eth1/11 Eth1/12 Eth1/13 Eth1/14 Eth1/15
                                        Eth1/16 Eth1/17 Eth1/18 Eth1/19 Eth1/20
                                        Eth1/21 Eth1/22 Eth1/23 Eth1/24 Eth1/25
                                        Eth1/26 Eth1/27 Eth1/28 Eth1/29 Eth1/30
                                        Eth1/31 Eth1/32 Eth1/33 Eth1/34 Eth1/35
                                        Eth1/36 Eth1/37 Eth1/38 Eth1/39 Eth1/40
                                        Eth1/41 Eth1/42 Eth1/43 Eth1/44 Eth1/45
                                        Eth1/46 Eth1/47 Eth1/48 Eth1/49 Eth1/50
Console#
```

Creating VLANs

Use the VLAN Static List to create or remove VLAN groups. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

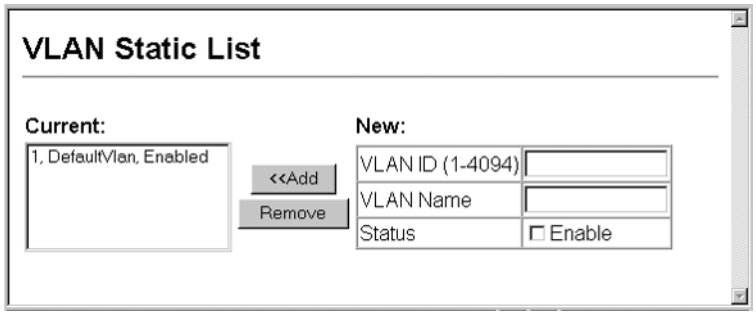
Command Attributes

- **Current** – Lists all the current VLAN groups created for this system. Up to 255 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.
- **New** – Allows you to specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)
- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Shows if this VLAN is enabled or disabled (Web).
  - **Enable**: VLAN is operational.
  - **Disable**: VLAN is suspended; i.e., does not pass packets.
- **State** – Shows if this VLAN is enabled or disabled (CLI).
  - **Active**: VLAN is operational.
  - **Suspend**: VLAN is suspended; i.e., does not pass packets.
- **Add** – Adds a new VLAN group to the current list.
- **Remove** – Removes a VLAN group from the current list. If any port is assigned to this group as untagged, it will be reassigned to VLAN group 1 as untagged.

Note: The maximum length of a VLAN name is 32 characters (the same as RFC2674 MIB definition). When a VLAN name is set through the ifAlias object (RFC2863 MIB), up to 64 characters can be used, but the name is always truncated to 32 characters, because both refer to the same database. The maximum lengths for all other names (such as ports and trunks) are 64 characters.

© 2004 Foundry Networks, Inc.

Web – Click VLAN, 802.1Q VLAN, Static List. Enter the VLAN ID and VLAN name, mark the Enable checkbox to activate the VLAN, and then click Add.



CLI – This example creates a new VLAN.

```
Console(config)#vlan                                              4-141
Console(config-vlan)#vlan 5 name R&D media ethernet state active  4-141
Console(config-vlan)#
```

Adding Interfaces Based on Membership Type

Use the VLAN Static Table to modify the settings for an existing VLAN. You can add or delete port members for a VLAN, disable or enable VLAN tagging for any port, or prevent a port from being automatically added to a VLAN via the GVRP protocol. (Note that VLAN 1 is the default untagged VLAN containing all ports on the switch, and cannot be modified via this page.)

You can use the VLAN Static Table to assign ports to the specified VLAN group as an IEEE 802.1Q tagged port. Assign ports as tagged if they are connected to 802.1Q VLAN-compliant devices. If the port is connected to VLAN-unaware devices, frames will be passed to the untagged VLAN group this port has been assigned to under the VLAN Port Configuration page.

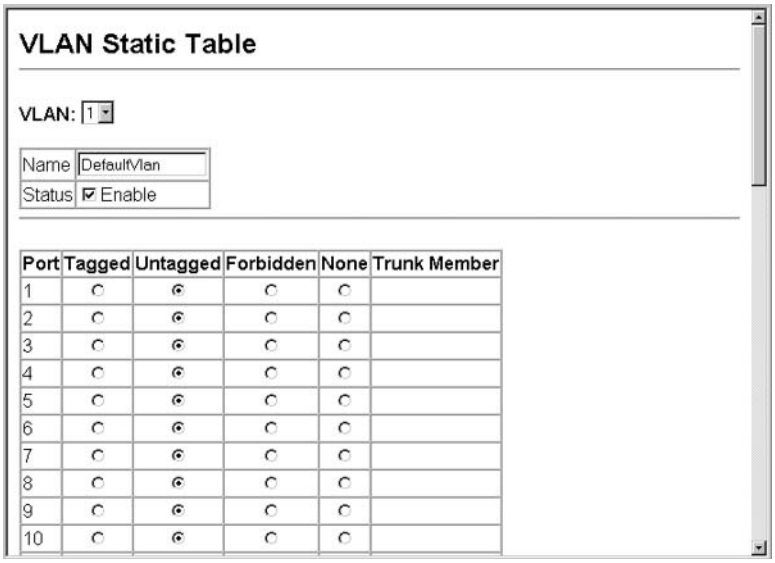
Command Attributes

- **Port** – Port identifier.
- **Trunk** – Trunk identifier.
- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes).
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Shows if this VLAN is enabled or disabled.
  - **Enable**: VLAN is operational.
  - **Disable**: VLAN is suspended; i.e., does not pass packets.

 © 2004 Foundry Networks, Inc.

- **Membership Type** – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
  - **Tagged**: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
  - **Untagged**: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
  - **Forbidden**: Interface is forbidden from automatically joining the VLAN via GVRP. For more information, see “Automatic VLAN Registration” on page 3-91.
  - **None**: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, 802.1Q VLAN, Static Table. Select a VLAN ID from the scroll-down list. Modify the VLAN name and status if required. Select the membership type by marking the appropriate radio button in the list of ports or trunks. Click Apply.


VLAN Static Table
VLAN: 1
Name DefaultVlan
Status Enable
Port Tagged Untagged Forbidden None Trunk Member
1 2 3 4 5 6 7 8 9 10

CLI – The following example shows how to add tagged and untagged ports to VLAN 2.

```
Console(config)#interface ethernet 1/1                          4-109
Console(config-if)#switchport allowed vlan add 2 tagged         4-147
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#switchport allowed vlan add 2 tagged
```

 © 2004 Foundry Networks, Inc.

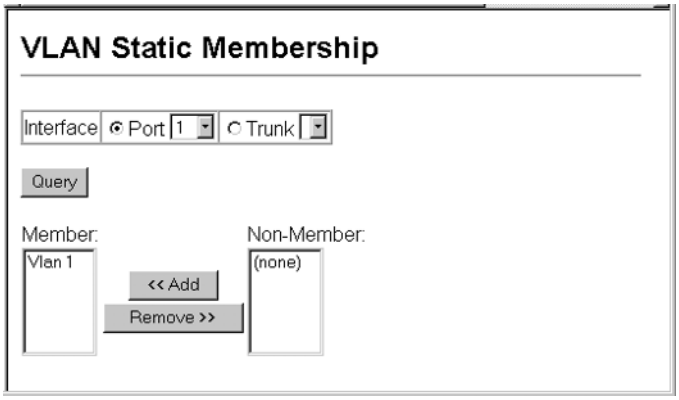
Adding Interfaces Based on Static Membership

Use the VLAN Static Membership by Port menu to assign VLAN groups to the selected interface add an interface to the selected VLAN as a tagged member.

Command Attributes

- **Interface** – Port or trunk identifier.
- **Member** – VLANs for which the selected interface is a tagged member.
- **Non-Member** – VLANs for which the selected interface is not a tagged member.

Web – Click VLAN, 802.1Q VLAN, Static Membership. Select an interface from the scroll-down box (Port or Trunk). Click Query to display VLAN membership information for the interface. Select a VLAN ID, and then click Add to add the interface as a tagged member, or click Remove to remove the interface. After configuring VLAN membership for each interface, click Apply.



CLI – This example adds Port 3 to VLAN 1 as a tagged port, and removes Port 3 from VLAN 2.

```
Console(config)#interface ethernet 1/3                    4-109
Console(config-if)#switchport allowed vlan add 1 tagged   4-147
Console(config-if)#switchport allowed vlan remove 2
```

Configuring VLAN Behavior for Interfaces

You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, and ingress filtering, GVRP status, and GARP timers.

Command Usage

- **GVRP** – GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network.
- **GARP** – Group Address Registration Protocol is used by GVRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GVRP registration/deregistration.

 © 2004 Foundry Networks, Inc.

Command Attributes

- **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)

  - If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.

- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Option: All, Tagged; Default: All)

- **Ingress Filtering** – If ingress filtering is enabled, incoming frames for VLANs which do not include this ingress port in their member set will be discarded at the ingress port. (Default: Disabled)

  - Ingress filtering only affects tagged frames.
  - If ingress filtering is disabled, the interface will flood incoming frames for VLANs which do not include this ingress port in their member set (except for those VLANs explicitly forbidden on this port).
  - If ingress filtering is enabled, the interface will discard incoming frames tagged for VLANs which do not include this ingress port in their member set.
  - Ingress filtering does not affect VLAN independent BPDU frames, such as STP. However, it does affect VLAN dependent BPDU frames, such as GMRP.

- **GVRP Status** – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect. (See “Port Configuration” on page 3-52.) When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Enabled)

- **GARP Join Timer*** – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)

- **GARP Leave Timer*** – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)

- **GARP LeaveAll Timer*** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. (Range: 500-18000 centiseconds; Default: 1000)

* GARP timer settings must follow this rule:
2 x (join timer) < leave timer < leaveAll timer

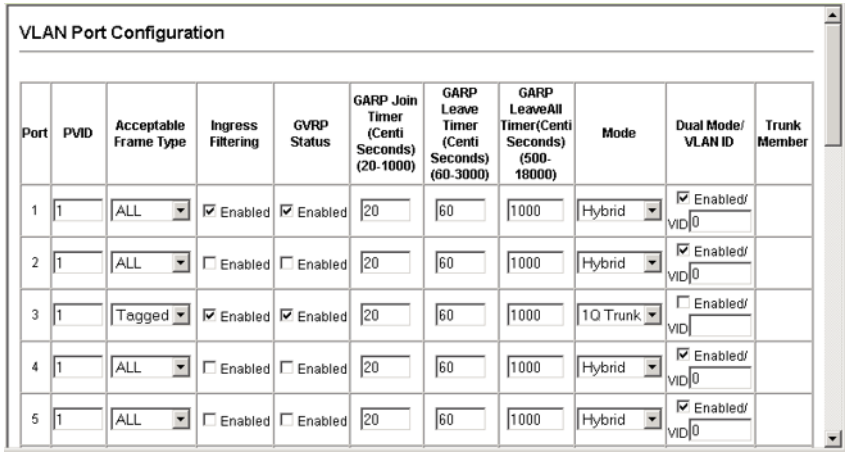
- **Mode** – Indicates VLAN membership mode for a port.
  (Default: Hybrid.)

  - **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port’s default VLAN (i.e.,associated with the PVID) are also transmitted as tagged frames.
  - **Hybrid** – Specifies a hybrid VLAN interface. The port may receive or transmit tagged or untagged frames.

 © 2004 Foundry Networks, Inc.

- **Dual Mode/VLAN ID** – Enables dual mode, the ability of a port to accept both tagged and untagged traffic at the same time. A dual mode port transmits only untagged traffic on its default VLAN (that is either VLAN 1, or a user specified VLAN ID), and only tagged traffic on all other VLANs. Allows you to specify a VLAN ID also. (Range: 1-4094; Default: 0)
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, 802.1Q VLAN, Port Configuration or VLAN Trunk Configuration. Fill in the required settings for each interface, click Apply.


VLAN Port Configuration
Port
PVID
Acceptable Frame Type
Ingress Filtering
GVRP Status
GARP Join Timer (Centi Seconds) (20-1000)
GARP Leave Timer (Centi Seconds) (60-3000)
GARP LeaveAll Timer(Centi Seconds) (500-18000)
Mode
Dual Mode/ VLAN ID
Trunk Member
1 1 ALL Enabled Enabled 20 60 1000 Hybrid Enabled/ VID 0
2 1 ALL Enabled Enabled 20 60 1000 Hybrid Enabled/ VID 0
3 1 Tagged Enabled Enabled 20 60 1000 1Q Trunk Enabled/ VID
4 1 ALL Enabled Enabled 20 60 1000 Hybrid Enabled/ VID 0
5 1 ALL Enabled Enabled 20 60 1000 Hybrid Enabled/ VID 0

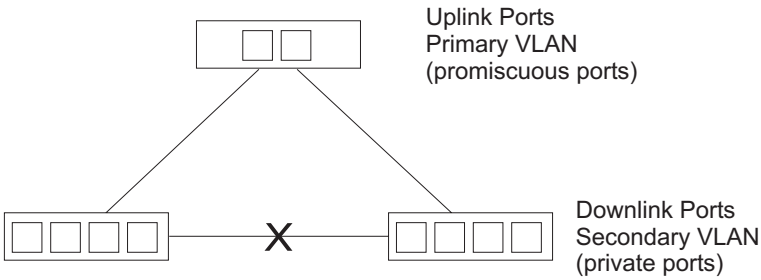
CLI – This example sets port 1 to accept only tagged frames, assigns PVID 3 as the native VLAN ID, enables GVRP, sets the GARP timers, sets the switchport mode to hybrid and then enables dual mode with a VLAN ID of 4000.

```
Console(config)#interface ethernet 1/1                        4-109
Console(config-if)#switchport acceptable-frame-types tagged  4-145
Console(config-if)#switchport ingress-filtering               4-145
Console(config-if)#switchport native vlan 3                   4-146
Console(config-if)#switchport gvrp                            4-154
Console(config-if)#garp timer join 10                         4-155
Console(config-if)#garp timer leave 90                        4-155
Console(config-if)#garp timer leaveall 2000                   4-155
Console(config-if)#switchport mode hybrid                     4-144
Console(config-if)#dual 4000
Console(config-if)#
```

 © 2004 Foundry Networks, Inc.

Configuring Private VLANs

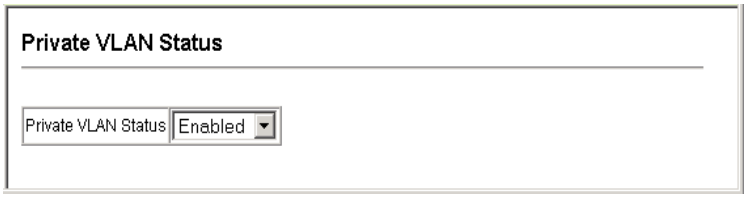
Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)



Enabling Private VLANs

Use the Private VLAN Status page to enable/disable the Private VLAN function.

Web – Click VLAN, Private VLAN, Status. Select Enable or Disable from the scroll-down box, and click Apply.



CLI – This example enables private VLANs.

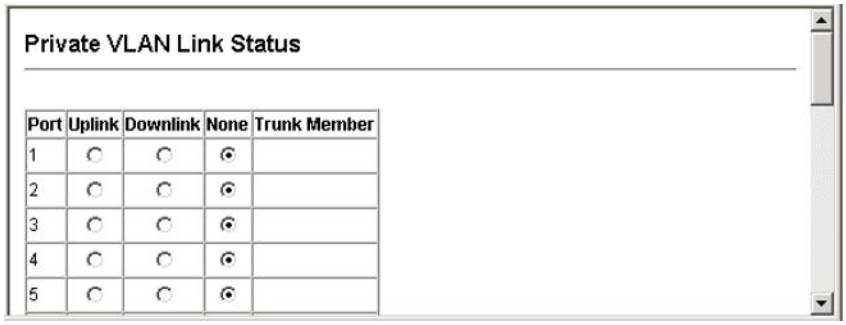
```
Console(config)#pvlan
Console(config)#
```

Configuring Uplink and Downlink Ports

Use the Private VLAN Link Status page to set ports as downlink or uplink ports. Ports designated as downlink ports can not communicate with any other ports on the switch except for the uplink ports. Uplink ports can communicate with any other ports on the switch and with any designated downlink ports.

© 2004 Foundry Networks, Inc.

Web – Click VLAN, Private VLAN, Link Status. Mark the ports that will serve as uplinks and downlinks for the private VLAN, then click Apply.



CLI – This configures ports 3 and 4 as uplinks and ports 5 and 6 as downlinks.

```
Console(config)#pvlan uplink 1/3-4 downlink 1/5-6
Console(config)#
```

Priority Configuration

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

Setting the Default Priority for Interfaces

You can specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

Command Usage

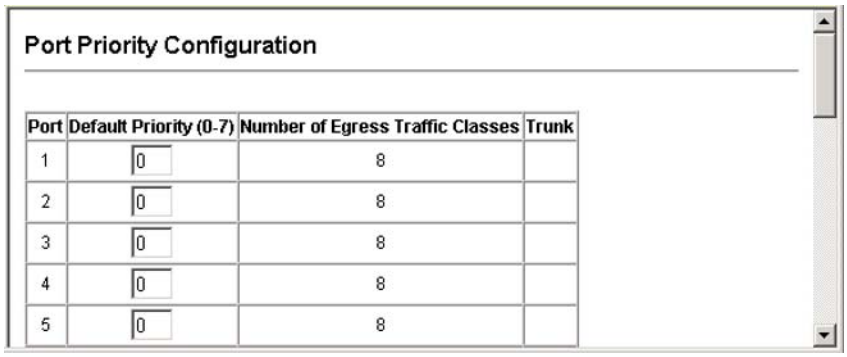
- This switch provides four priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage.
- The default priority applies if the incoming frame is an untagged frame received from a VLAN trunk or a static-access port. This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

Command Attributes

- **Default Priority** – The priority that is assigned to untagged frames received on the specified port. (Range: 0 - 7, Default: 0)
- **Number of Egress Traffic Classes** – The number of queue buffers provided for each port.

 © 2004 Foundry Networks, Inc.

Web – Click Priority, Default Port Priority or Default Trunk Priority. Modify the default priority for any interface, then click Apply.



CLI – This example assigns a default priority or 5 to port 3.

```
Console(config)#interface ethernet 1/3                    4-109
Console(config-if)#switchport priority default 5          4-144
```

Mapping CoS Values to Egress Queues

This switch processes Class of Service (CoS) priority tagged traffic by using four priority queues for each port, with service schedules based on Weighted Round Robin (WRR). Up to eight separate traffic priorities are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

	Queue			
	0	**1**	**2**	**3**
Priority		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

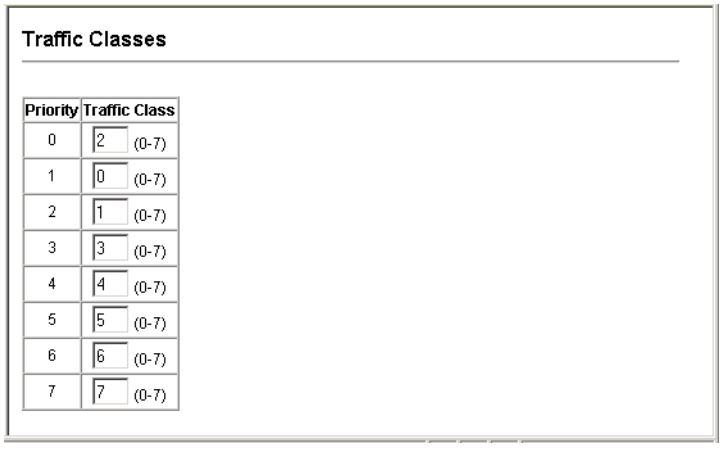
© 2004 Foundry Networks, Inc.

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table. However, you can map the priority levels to the switch's output queues in any way that benefits application traffic for your own network.

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

- **Priority** – CoS value. (Range: 0 to 7, where 7 is the highest priority)
- **Traffic Class** – Output queue buffer.

Web – Click Priority, Traffic Classes. Assign priorities to the output queues, then click Apply.



 © 2004 Foundry Networks, Inc.

CLI – The following example shows how to map CoS values 0, 1 and 2 to CoS priority queue 0, value 3 to CoS priority queue 1, values 4 and 5 to CoS priority queue 2, and values 6 and 7 to CoS priority queue 3.

```
Console(config)#interface ethernet 1/1                          4-109
Console(config)#queue cos-map 0 0 1 2                           4-167
Console(config)#queue cos-map 1 3
Console(config)#queue cos-map 2 4 5
Console(config)#queue cos-map 3 6 7
Console(config)#exit
Console#show queue cos-map ethernet 1/1                         4-168
Information of Eth 1/1
 Queue ID Traffic class
 -------- -------------
    0     0 1 2
    1     3
    2     4 5
    3     6 7
Console#
```

Setting the Service Weight for Traffic Classes

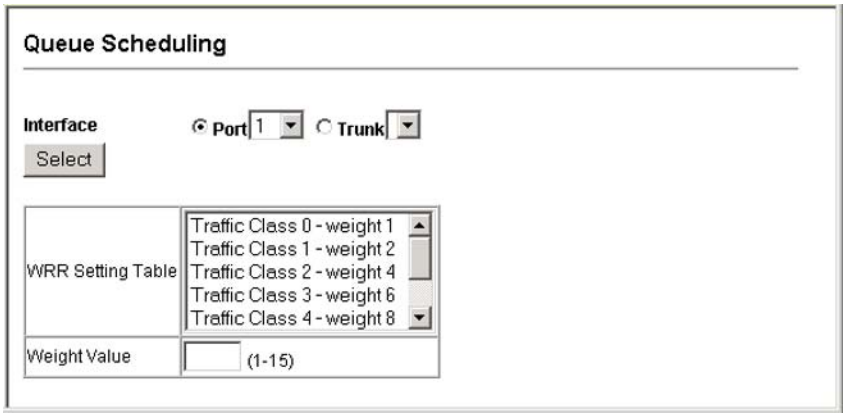
This switch uses the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each priority queue. As described in “Mapping CoS Values to Egress Queues” on page 3-103, the traffic classes are mapped to one of the four egress queues provided for each port. You can assign a weight to each of these queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue will be polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

Command Attributes

- **Interface** – Specifies a port or trunk.
- **WRR Setting Table** – Displays a list of weights for each traffic class (i.e., queue).
  - EdgeIron 4802CF, 2402CF – Defaults: Weights 1, 4, 16 and 64 are assigned to queue 0, 1, 2 and 3 respectively.
  - EdgeIron 24G-A, 48G – Defaults: Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queue 0, 1, 2, 3, 4, 5, 6 and 7 respectively.
  - EdgeIron 24G – Defaults: Weights 16, 64, 128 and 240 are assigned to queue 0, 1, 2 and 3 respectively.
- **Weight Value** – Set a new weight for the selected traffic class.

 © 2004 Foundry Networks, Inc.

Web – Click Priority, Queue Scheduling. Select a traffic class by clicking on it with your cursor, enter a weight value, and then click Apply.



CLI – The following example shows how to assign WRR weights of 1, 4, 16 and 64 to the CoS priority queues 0, 1, 2 and 3.

```
Console(config)#queue bandwidth 1 4 16 64                    4-166
Console(config)#exit
Console#show queue bandwidth                                 4-168
 Queue ID Weight
 -------- ------
        0      1
        1      4
        2     16
        3     64
Console#
```

Mapping Layer 3/4 Priorities to CoS Values

This switch supports a common method of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet or the number of the TCP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner:

- The precedence for priority mapping is IP Port priority, IP Precedence or DSCP Priority, and then Default Port Priority.
- IP Precedence and DSCP Priority cannot both be enabled. Enabling one of these priority types will automatically disable the other.
- IP Port, IP Precedence, and DSCP Priority settings are global and apply to all ports on the switch.

Note: IP Precedence/DSCP and TCP port priority to COS mappings are global settings.

© 2004 Foundry Networks, Inc.

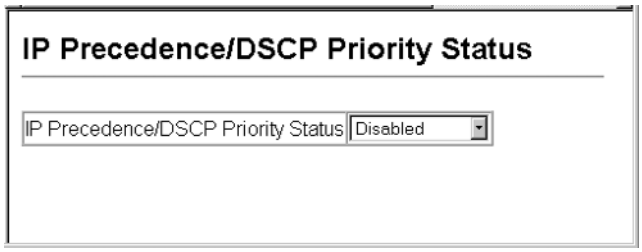
Selecting IP Precedence/DSCP Priority

The switch allows you to choose between using IP Precedence or DSCP priority. Select one of the methods or disable this feature.

Command Attributes

- **IP Precedence/DSCP Priority Status** – Selects IP Precedence, DSCP, or disables both priority services.

Web – Click Priority, IP Precedence Priority. Select IP Precedence or IP DSCP from the IP Precedence/DSCP Priority Status menu.



CLI – The following example globally enables IP Precedence service on the switch.

```
Console(config)#map ip precedence                              4-169
Console#
```

Mapping IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The default IP Precedence values are mapped one-to-one to Class of Service values (i.e., Precedence value 0 maps to CoS value 0, and so forth). Bits 6 and 7 are used for network control, and the other bits for various application types. ToS bits are defined in the following table.

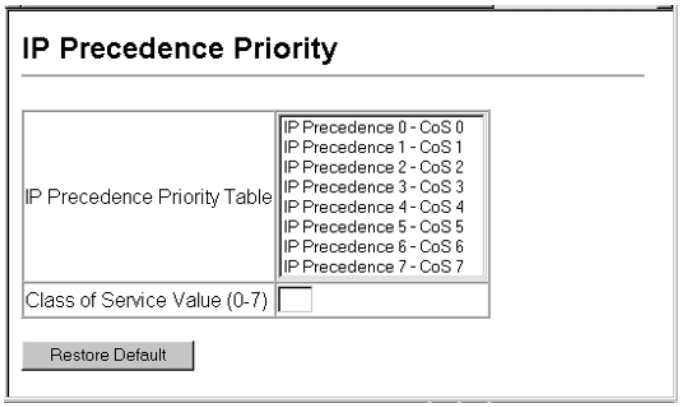
Priority Level	Traffic Type
7	Network Control
6	Internetwork Control
5	Critical
4	Flash Override
3	Flash
2	Immediate
1	Priority
0	Routine

© 2004 Foundry Networks, Inc.

Command Attributes

- **IP Precedence Priority Table** – Shows the IP Precedence to CoS map.
- **Class of Service Value** – Maps a CoS value to the selected IP Precendence value. Note that "0" represents low priority and "7" represent high priority.

Web – Click Priority, IP Precedence Priority. Select an IP Precedence value from the IP Precedence Priority Table by clicking on it with your cursor, enter a value in the Class of Service Value field, and then click Apply. Be sure to also select IP Precedence from the IP Precedence/DSCP Priority Status menu.


IP Precedence Priority
IP Precedence Priority Table
IP Precedence 0 - CoS 0
IP Precedence 1 - CoS 1
IP Precedence 2 - CoS 2
IP Precedence 3 - CoS 3
IP Precedence 4 - CoS 4
IP Precedence 5 - CoS 5
IP Precedence 6 - CoS 6
IP Precedence 7 - CoS 7
Class of Service Value (0-7)
Restore Default

CLI – The following example globally enables IP Precedence service on the switch, maps IP Precedence value 1 to CoS value 0 on port 5, and then displays all the IP Precedence settings for that port. (Note that the setting is global and applies to all ports on the switch.)

```
Console(config)#map ip precedence                              4-169
Console(config)#interface ethernet 1/5                         4-109
Console(config-if)#map ip precedence 1 cos 0                   4-169
Console(config-if)#end
Console#show map ip precedence ethernet 1/5                    4-173
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 5          0   0
  Eth 1/ 5          1   0
  Eth 1/ 5          2   2
  Eth 1/ 5          3   3
  Eth 1/ 5          4   4
  Eth 1/ 5          5   5
  Eth 1/ 5          6   6
  Eth 1/ 5          7   7
Console#
```


© 2004 Foundry Networks, Inc.

Mapping DSCP Priority

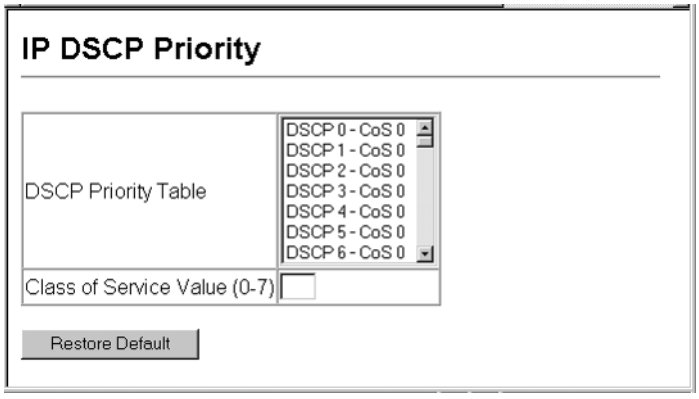
The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, and it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Attributes

- **DSCP Priority Table –** Shows the DSCP Priority to CoS map.
- **Class of Service Value –** Maps a CoS value to the selected DSCP Priority value. Note that “0” represents low priority and “7” represent high priority.

Web – Click Priority, IP DSCP Priority. Select a DSCP priority value from the DSCP Priority Table by clicking on it with your cursor, enter a value in the Class of Service Value field, and then click Apply. Be sure to also select IP DSCP from the IP Precedence/DSCP Priority Status menu.


IP DSCP Priority
DSCP Priority Table
DSCP 0 - CoS 0
DSCP 1 - CoS 0
DSCP 2 - CoS 0
DSCP 3 - CoS 0
DSCP 4 - CoS 0
DSCP 5 - CoS 0
DSCP 6 - CoS 0
Class of Service Value (0-7)
Restore Default

© 2004 Foundry Networks, Inc.

CLI – The following example globally enables DSCP Priority service on the switch, maps DSCP value 1 to CoS value 0 on port 5, and then displays all the DSCP Priority settings for that port. (Note that the setting is global and applies to all ports on the switch.)

```
Console(config)#map ip dscp                                    4-170
Console(config)#interface ethernet 1/5                         4-109
Console(config-if)#map ip dscp 1 cos 0                         4-171
Console(config-if)#end
Console#show map ip dscp ethernet 1/5                          4-173
DSCP mapping status: disabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 5    0   0
  Eth 1/ 5    1   0
  Eth 1/ 5    2   0
  Eth 1/ 5    3   0
.
.
.
  Eth 1/ 5   61   0
  Eth 1/ 5   62   0
  Eth 1/ 5   63   0
Console#
```

Mapping IP Port Priority

You can also map network applications to Class of Service values based on the IP port number (i.e., TCP/UDP port number) in the frame header. Some of the more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

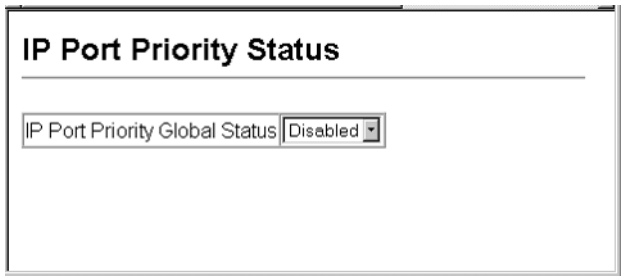
Command Attributes

- **IP Port Priority Status** – Enables or disables the IP port priority.
- **Interface** – Selects the port or trunk interface to which the settings apply.
- **IP Port Priority Table** – Shows the IP port to CoS map.
- **IP Port Number (TCP/UDP)** – Set a new IP port number.
- **Class of Service Value** – Sets a CoS value for a new IP port. Note that “0” represents low priority and “7” represent high priority.

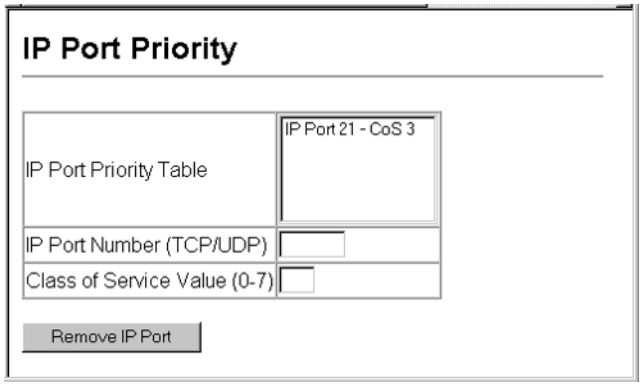
Note: CoS priority mappings are configured per-port. However, due to a hardware limitations all mappings are applied system-wide. In other words, no matter which port is set for CoS mapping, it’s applies globally to all ports.

© 2004 Foundry Networks, Inc.

Web – Click Priority, IP Port Status. Set IP Port Priority Status to Enabled.



Click Priority, IP Port Priority. Select a port or trunk from the Interface field (note that settings apply to all interfaces). Enter the port number for a network application in the IP Port Number box and the new CoS value in the Class of Service box, and then click Add IP Port.



CLI – The following example globally enables IP Port Priority service on the switch, maps HTTP traffic (on port 5) to CoS value 0, and then displays the IP Port Priority settings.

```
Console(config)#map ip port                                    4-172
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0                        4-172
Console(config-if)#end
Console#show map ip port ethernet 1/5                          4-174
TCP port mapping status: enabled

 Port      Port no. COS
 --------- -------- ---
  Eth 1/ 5       80   0
Console#
```

Note: Mapping specific values for IP Port Priority is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

© 2004 Foundry Networks, Inc.

Mapping CoS Values to ACLs

Use the ACL CoS Mapping page to set the output queue for packets matching an ACL rule as shown in the following table. Note that the specified CoS value is only used to map the matching packet to an output queue; it is not written to the packet itself. For information on mapping the CoS values to output queues, see page 33-103.

Priority	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Usage

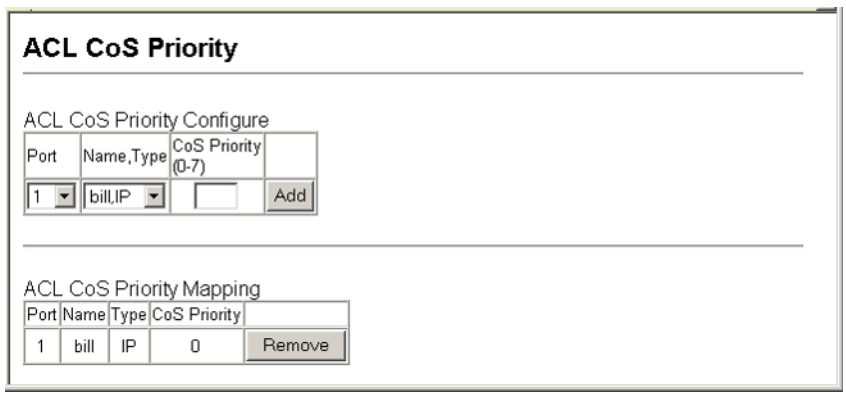
You must configure an ACL mask before you can map CoS values to the rule.

Command Attributes

- **Port** – Selects the port to which the ACL CoS is configured on.
- **Name, Type** – Not presently implemented.
- **CoS Priority** – Enables the CoS priority value level.
- **Add** – Adds the specified information to the port.
- **ACL CoS Priority Mapping** – Displays the configured information.

* For information on configuring ACLs, see page 33-40.

Web – Click Priority, ACL CoS Priority. Select a port, select an ACL rule, specify a CoS priority, then click Add.



 © 2004 Foundry Networks, Inc.

CLI – This example assigns a CoS value of zero to packets matching rules within the specified ACL on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#map access-list ip bill cos 0
Console(config-if)#
```

Changing Priorities Based on ACL Rules

You can change traffic priorities for frames matching the defined ACL rule. (This feature is commonly referred to as ACL packet marking.) This switch can change the IEEE 802.1p priority, IP Precedence, or DSCP Priority of IP frames; or change the IEEE 802.1p priority of Layer 2 frames. (This feature is commonly referred to as ACL packet marking.) Use the no form to remove the ACL marker.

Command Usage

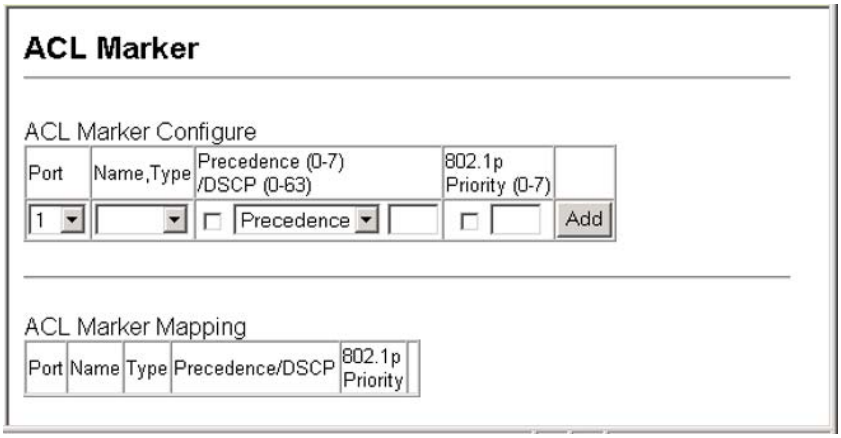
- You must configure an ACL mask before you can change priorities based on a rule.
- Traffic priorities may be included in the IEEE 802.1p priority tag. This tag is also incorporated as part of the overall IEEE 802.1Q VLAN tag. The 802.1p priority may be set for either Layer 2 or IP frames.
- The IP frame header also includes priority bits in the Type of Service (ToS) octet. The Type of Service octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. Note that the IP frame header can include either the IP Precedence or DSCP priority type.
- The precedence for priority mapping by this switch is IP Precedence or DSCP Priority, and then 802.1p priority.

Command Attributes

- **Port** – Port identifier.
- **Name*** – Name of ACL.
- **Type** – Type of ACL (IP or MAC).
- **Precedence** – IP Precedence value. (Range: 0-7)
- **DSCP** – Differentiated Services Code Point value. (Range: 0-63)
- **802.1p Priority** – Class of Service value in the IEEE 802.1p priority tag. (Range: 0-7; 7 is the highest priority)

© 2004 Foundry Networks, Inc.

Web – Click Priority, ACL Marker. Select a port and an ACL rule. To specify a ToS priority, mark the Precedence/DSCP check box, select Precedence or DSCP from the scroll-down box, and enter a priority. To specify an 802.1p priority, mark the 802.1p Priority check box, and enter a priority. Then click Add.



CLI – This example changes the DSCP priority for packets matching an IP ACL rule, and the 802.1p priority for packets matching a MAC ACL rule.

```
Console(config)#interface ethernet 1/1
Console(config-if)#match access-list ip bill set dscp 0
Console(config-if)#match access-list mac mike set priority 0
Console(config-if)#end
Console#show marking                                          4-80
Interface ethernet 1/1
 match access-list IP bill set DSCP 0
 match access-list MAC a set priority 0
Console#
```

Multicast Configuration

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on the hosts which subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. This procedure is called multicast filtering.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

 © 2004 Foundry Networks, Inc.

Configuring IGMP Parameters

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

Command Usage

- **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures multicast filters accordingly.
- **IGMP Query** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any adjacent multicast switch/router to ensure that it will continue to receive the multicast service.

Note: Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Command Attributes

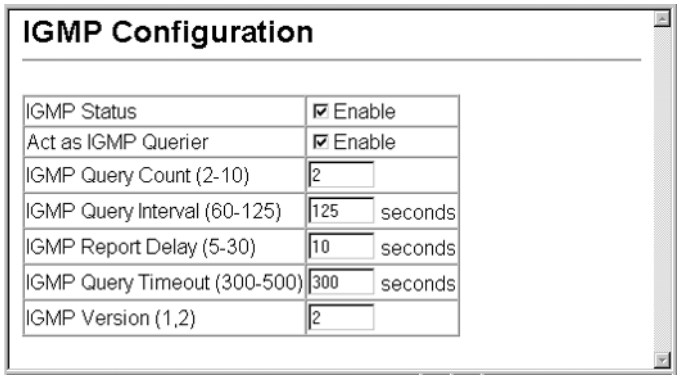
- **IGMP Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping. (Default: Disabled)
- **Act as IGMP Querier** – When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled)
- **IGMP Query Count** – Sets the maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Default: 2, Range: 2 - 10)
- **IGMP Query Interval** – Sets the frequency (in seconds) at which the switch sends IGMP host-query messages. (Default: 125, Range: 60 - 125)
- **IGMP Report Delay** – Sets the time (in seconds) between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Default: 10, Range: 5 - 30)
- **Query Timeout** – The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. (Default: 300 seconds, Range: 300 - 500)
- **IGMP Version** – Sets the protocol version for compatibility with other devices on the network. (Default: 2, Range: 1 - 2)

Notes: 1. All systems on the subnet must support the same version.

2. Some attributes are only enabled for IGMPv2, including IGMP Report Delay and IGMP Query Timeout.

© 2004 Foundry Networks, Inc.

Web – Click IGMP, IGMP Configuration. Adjust the IGMP settings as required, and then click Apply. (The default settings are shown below.)



CLI – This example modifies the settings for multicast filtering, and then displays the current status.

```
Console(config)#ip igmp snooping                              4-158
Console(config)#ip igmp snooping querier                      4-160
Console(config)#ip igmp snooping query-count 10               4-161
Console(config)#ip igmp snooping query-interval 100           4-161
Console(config)#ip igmp snooping query-max-response-time 20   4-162
Console(config)#ip igmp snooping router-port-expire-time 300 4-163
Console(config)#ip igmp snooping version 2                    4-159
Console(config)#exit
Console#show ip igmp snooping                                 4-159
 Igmp Snooping Configuration
 ---------------------------------------------
 Service status          : Enabled
 Querier status          : Enabled
 Query count             : 10
 Query interval          : 100 sec
 Query max response time : 20 sec
 Query time-out          : 300 sec
 IGMP snooping version   : Version 2
Console#
```

Interfaces Attached to a Multicast Router

Multicast routers use the information obtained from IGMP Query, along with a multicast routing protocol such as DVMRP, to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch.

You can use the Multicast Router Port Information page to display the ports on this switch attached to a neighboring multicast router/switch for each VLAN ID.

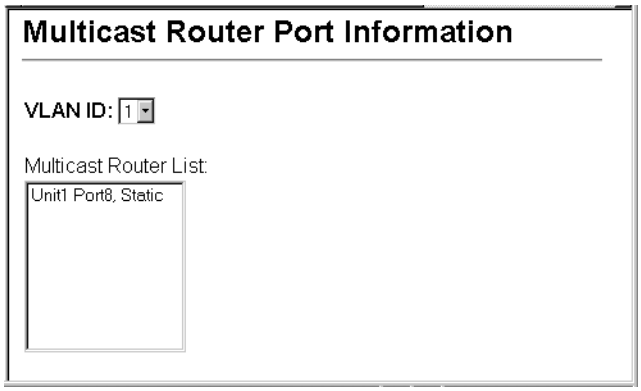
Displaying Interfaces Attached to a Multicast Router

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094).
- **Multicast Router List** – Multicast routers dynamically discovered by this switch or those that are statically assigned to an interface on this switch.

 © 2004 Foundry Networks, Inc.

Web – Click IGMP, Multicast Router Port Information. Select the required VLAN ID from the scroll-down list to display the associated multicast routers.



CLI – This example shows that Port 11 has been statically configured as a port attached to a multicast router.

```
Console#show ip igmp snooping mrouter vlan 1                    4-164
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1           Eth 1/11 Static
```

Specifying Interfaces Attached to a Multicast Router

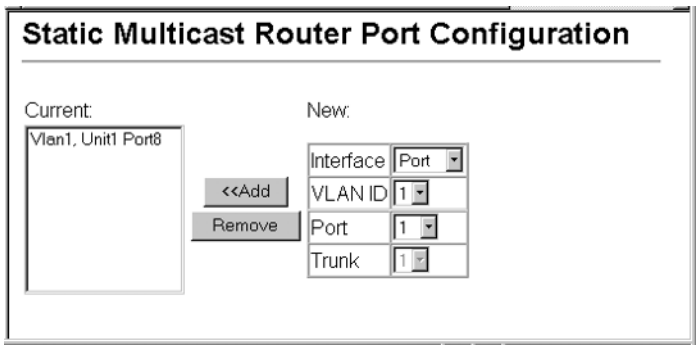
Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your switch, you can manually configure that interface to join all the current multicast groups. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

Command Attributes

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/switch.
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

© 2004 Foundry Networks, Inc.

Web – Click IGMP, Static Multicast Router Port Configuration. Specify the interfaces attached to a multicast router, indicate the VLAN which will forward all the corresponding multicast traffic, and then click Add. After you have completed adding interfaces to the list, click Apply.



CLI – This example configures port 11 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11 4-163
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1                  4-164
 VLAN M'cast Router Port Type
 ---- ----------------- -------
    1           Eth 1/11  Static
```

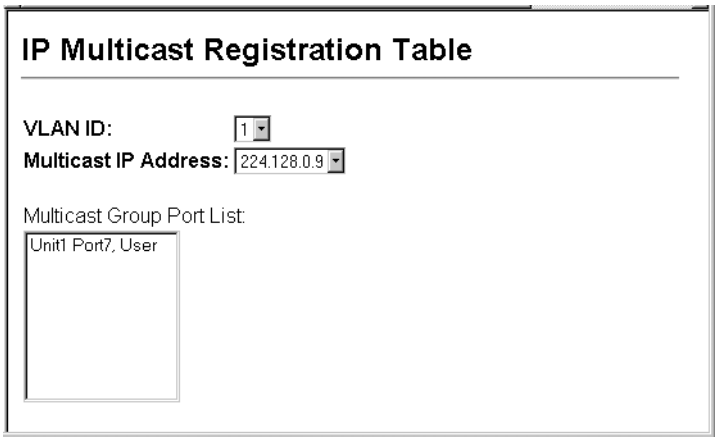
Displaying Port Members of Multicast Services

You can display the port members associated with a specified VLAN and multicast IP address.

Command Attributes

- **VLAN ID** – Selects the VLAN in which to display port members.
- **Multicast IP Address** – The IP address for a specific multicast service
- **Multicast Group Port List** – Ports propagating a multicast service; i.e., ports that belong to the indicated VLAN group.

Web – Click IGMP, IP Multicast Registration Table. Select the VLAN ID and multicast IP address. The switch will display all the ports that are propagating this multicast service.



© 2004 Foundry Networks, Inc.

CLI – This example displays all the known multicast services supported on VLAN 1, along with the ports propagating the corresponding services. The type field shows if this entry was learned dynamically or was statically configured.

```
Console#show mac-address-table multicast vlan 1              4-160
 VLAN M'cast    IP addr.     Member ports  Type
 ---- --------  -------      ------------  -------
    1          224.0.0.12   Eth1/12       USER
    1          224.1.2.3    Eth1/12       IGMP
Console#
```

Adding Multicast Addresses to VLANs

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in “Configuring IGMP Parameters” on page 3-115. For certain application that require tighter control, you may need to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

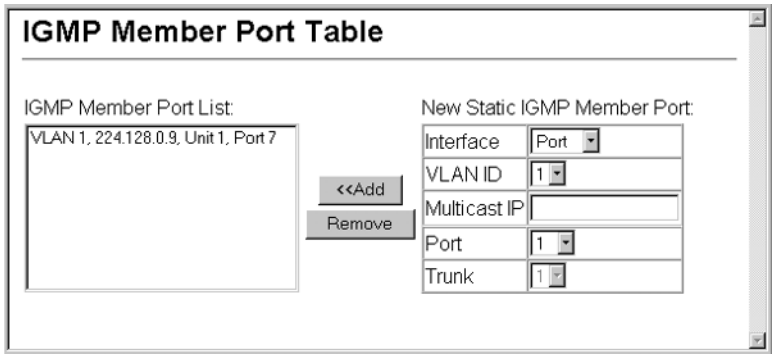
Command Usage

- Static multicast addresses are never aged out.
- When a multicast address is assigned to specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Command Attributes

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/switch.
- **Multicast IP** – The IP address for a specific multicast service
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

Web – Click IGMP, IGMP Member Port Table. Specify the interface attached to a multicast service (via an IGMP-enabled switch or multicast router), indicate the VLAN that will propagate the multicast service, specify the multicast IP address, and then click Add. After you have completed adding ports to the member list, click Apply.



 © 2004 Foundry Networks, Inc.

CLI – This example assigns a multicast address to VLAN 1, and then displays all the known multicast services supported on VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/12  4-158
Console(config)#exit
Console#show mac-address-table multicast vlan 1                          4-160
 VLAN M'cast      IP addr.      Member ports     Type
 ---- --------    -------       ------------     -------
    1             224.0.0.12    Eth1/12          USER
    1             224.1.2.3     Eth1/12          IGMP
Console#
```

Showing Device Statistics

You can display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMOM MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.

Note: RMON groups 2, 3 and 9 can only be accessed using SNMP management software.

Statistical Values

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Received Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Received Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmit Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmit Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

 © 2004 Foundry Networks, Inc.

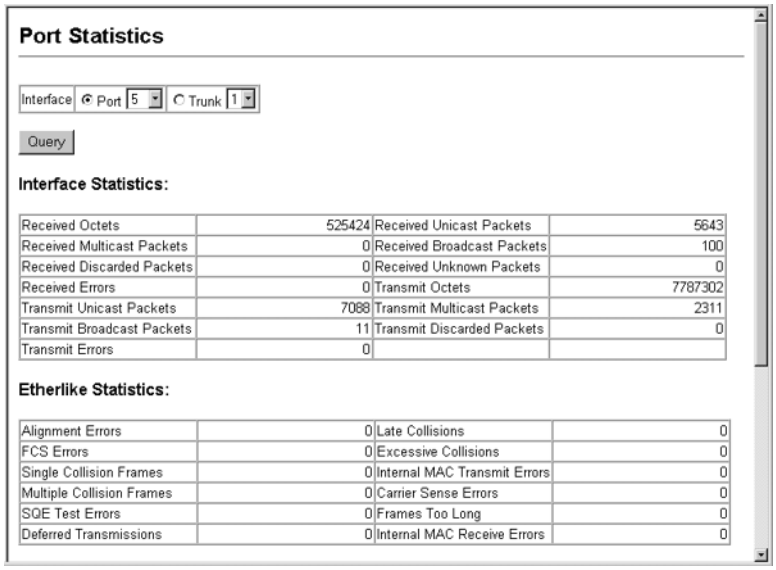
Parameter	Description
Transmit Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmit Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Transmit Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Transmit Errors	The number of outbound packets that could not be transmitted because of errors.
Etherlike Statistics	
Alignment Errors	The number of alignment errors (missynchronized data packets).
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
RMON Statistics	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.

© 2004 Foundry Networks, Inc.

Parameter	Description
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

 © 2004 Foundry Networks, Inc.

Web – Click Statistics, Port Statistics. Select the required interface, and then click Query. You can also use the Refresh button at the bottom of the page to update the screen.



Port Statistics

Interface ◉ Port 5 ○ Trunk 1

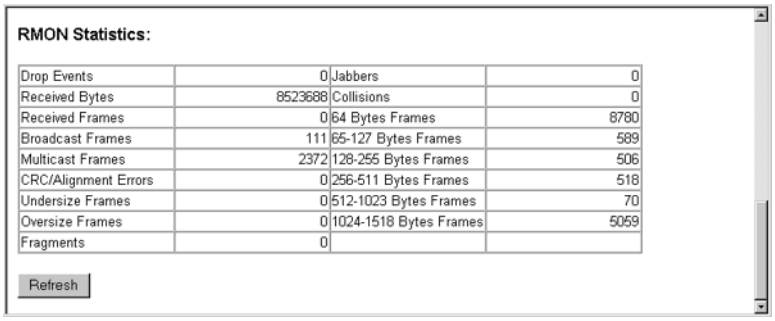
Query

Interface Statistics:

Received Octets	525424	Received Unicast Packets	5643
Received Multicast Packets	0	Received Broadcast Packets	100
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	7787302
Transmit Unicast Packets	7088	Transmit Multicast Packets	2311
Transmit Broadcast Packets	11	Transmit Discarded Packets	0
Transmit Errors	0		

Etherlike Statistics:

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0



RMON Statistics:

Drop Events	0	Jabbers	0
Received Bytes	8523688	Collisions	0
Received Frames	0	64 Bytes Frames	8780
Broadcast Frames	111	65-127 Bytes Frames	589
Multicast Frames	2372	128-255 Bytes Frames	506
CRC/Alignment Errors	0	256-511 Bytes Frames	518
Undersize Frames	0	512-1023 Bytes Frames	70
Oversize Frames	0	1024-1518 Bytes Frames	5059
Fragments	0		

Refresh

© 2004 Foundry Networks, Inc.

CLI – This example shows statistics for port 13.

```
Console#show interfaces counters ethernet 1/13                                    4-118
Ethernet 1/13
 Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unitcast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets: 871
Console#
```

 © 2004 Foundry Networks, Inc.

Chapter 4
Command Line Interface

This chapter describes how to use the Command Line Interface (CLI).

Using the Command Line Interface

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are "admin" and "guest" with corresponding passwords of "admin" and "guest.") When the administrator user name and password is entered, the CLI displays the "Console#" prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the "Console>" prompt and enters normal access mode (i.e., Normal Exec).
2. Enter the necessary commands to complete your desired tasks.
3. When finished, exit the session with the "quit" or "exit" command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification

Username: admin
Password:

      CLI session with the EdgeIron 4802CF is opened.
      To end the CLI session, enter [Exit].

Console#
```

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a

© 2004 Foundry Networks, Inc.

network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

To access the switch through a Telnet session, you must first set the IP address for the switch, and set the default gateway if you are managing the switch from a different IP subnet. For example:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.1 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps.

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the “Vty-0#” prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or “Vty-0>” for the guest to show that you are using normal access mode (i.e., Normal Exec).
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the “quit” or “exit” command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

      CLI session with the EdgeIron 4802CF is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

Note: You can open up to four sessions to the device via Telnet.

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “show interfaces status ethernet 1/5,” **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

 © 2004 Foundry Networks, Inc.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

```
Console>enable
Console#show startup-config
```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)#username admin password 0 smith
```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command “configure” can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the “configure” example, typing **con** followed by a tab will result in printing the command up to “**configure**.”

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the “?” character to list keywords or parameters.

Showing Commands

If you enter a “?” at the command prompt, the system will display the first level of keywords for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, Interface,

 © 2004 Foundry Networks, Inc.

Line, or VLAN Database). You can also display a list of valid keywords for a specific command. For example, the command "**show ?**" displays a list of possible show commands:

```
Console#show ?
  access-group       Access groups
  access-list        Access lists
  bridge-ext         Bridge extend information
  calendar           Date information
  dot1x              Show 802.1x content
  garp               Garp property
  gvrp               Show gvrp information of interface history
  history            Information of history
  interfaces         Information of interfaces
  ip                 IP information
  lacp               Show lacp statistic
  line               TTY line information
  logging            Show the contents of logging buffers
  mac                MAC access lists
  mac-address-table  Set configuration of the address table
  management         Show management ip filter
  map                Map priority
  marking            Specify marker
  port               Characteristics of the port
  public-key         Show information of public key
  pvlan              Information of private VLAN
  queue              Information of priority queue
  radius-server      Radius server information
  running-config     The system configuration of running
  snmp               SNMP statistics
  sntp               SNTP
  spanning-tree      Specify spanning-tree
  ssh                Secure shell
  startup-config     The system configuration of starting up
  system             Information of system
  tacacs-server      Login by tacacs server
  users              Display information about terminal lines
  version            System hardware and software status
  vlan               Switch VLAN Virtual Interface
Console#show
```

The command "**show interfaces ?**" will display the following information:

```
Console>show interfaces ?
  counters    Information of interfaces counters
  status      Information of interfaces status
  switchport  Information of interfaces switchport
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example "**s?**" shows all the keywords starting with "s."

```
Console#show s?
snmp            sntp      spanning-tree   ssh      startup-config      system
Console#show s
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword "**no**" to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

© 2004 Foundry Networks, Inc.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark "**?**" at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Class	Mode
Exec	Normal Privileged
Configuration*	Global Interface Line VLAN

* You must be in Privileged Exec mode to access any of the configuration modes.

Exec Commands

When you open a new console session on switch with the user name "guest," the system enters Normal Exec command mode (or guest mode). Only a limited number of the commands are available in this mode. You can access all the commands only in Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name "admin," or enter the **enable** command (followed by the privileged level password if so configured). The command prompt displays as "Console>" for Normal Exec mode and "Console#" for Privileged Exec mode.

© 2004 Foundry Networks, Inc.

To enter Privileged Exec mode, enter the following commands and passwords:

```
Username: admin
Password: [system login password]

      CLI session with the EdgeIron 4802CF is opened.
      To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [system login password]

      CLI session with the EdgeIron 4802CF is opened.
      To end the CLI session, enter [Exit].

Console#enable
Password: [privileged level password if so configured]
Console#
```

Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in nonvolatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into three different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port configuration, and include command such as **parity** and **databits**.
- VLAN Configuration - Includes the command to create VLAN groups.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to “Console(config)#” which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```

To enter Interface, Line Configuration, or VLAN mode, you must enter the “**interface** ...,” “**line**...” or “**vlan database**” command while in Global Configuration mode. The system prompt will change to “Console(config-if)#,” “Console(config-line)#” or Console(config-vlan)” indicating that you have access privileges to the associated commands. You can use the **end** command to return to the Privileged Exec mode.

```
Console(config)#interface ethernet 1/5
Console(config-if)#exit
Console(config)#line console
Console(config-line)#
```

 © 2004 Foundry Networks, Inc.

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the "?" character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-P	Shows the last command.
Ctrl-U	Deletes the entire line.
Ctrl-W	Deletes the last word typed.
Delete key or backspace key	Erases a mistake when entering a command.

Command Groups

The system commands can be broken down into the functional groups shown below.

Command Group	Description	Page
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	4-8
Flash/File	Manages code image or switch configuration files	4-13
System Management	Controls system logs, system passwords, user name, browser management options, HTTPS, SSH 2.0, and a variety of other system information	4-18
SNTP	Configures clock settings for SNTP and NTP clients.	4-51
Authentication	Configures RADIUS and TACACS+ client-server authentication for logon access; also configures IEEE 802.1x port access control	4-56
ACL	Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or non-IP frames (based on MAC address or Ethernet type)	4-67
SNMP	Activates authentication failure traps; configures community access strings, and trap managers	4-91
IP	Configures the IP address and gateway for management access, displays the default gateway, or pings a specified device	4-96
Line	Sets communication parameters for the serial port, including baud rate and console time-out.	4-101
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	4-108

© 2004 Foundry Networks, Inc.

Command Group	Description	Page
Address Table	Configures the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time	4-121
Spanning Tree	Configures spanning tree settings for the switch	4-124
VLAN	Configures VLAN settings, and defines port membership for VLAN groups	4-140
PVLAN	Enables or configures private VLANs	4-149
GVRP and Bridge Extension	Configures GVRP settings that permit automatic VLAN learning; Shows the configuration for bridge extension MIB	4-153
IGMP Snooping	Configures IGMP multicast filtering, querier eligibility, query parameters, and specifies ports attached to a multicast router	4-157
Priority	Sets port priority for untagged frames, relative weight for each priority queue, also sets priority for IP precedence and DSCP	4-164
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	4-175
Port Trunking and LACP	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	4-177
Rate Limiting	Controls the maximum rate for traffic transmitted or received on a port	4-186

Note that the access mode shown in the following tables is indicated by these abbreviations:

NE (Normal Exec)
PE (Privileged Exec)
GC (Global Configuration)
IC (Interface Configuration)
LC (Line Configuration)
VC (VLAN Database Configuration)

General Commands

Command	Function	Mode	Page
enable	Activates privileged mode	NE	4-9
disable	Returns to normal mode from privileged mode	PE	4-9
configure	Activates global configuration mode	PE	4-10
reload	Restarts the system	PE	4-11
prompt	Customizes the CLI prompt	GC	4-12
end	Returns to Privileged Exec mode	GC, IC, LC, VC	4-12
exit	Returns to the previous configuration mode, or exits the CLI	any	4-12
quit	Exits a CLI session	NE, PE	4-13
help	Shows how to use help	any	NA
?	Shows options for command completion (context sensitive)	any	NA

© 2004 Foundry Networks, Inc.

enable

Use this command to activate Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See “Understanding Command Modes” on page 4-5.

Syntax

enable [*level*]

level - Privilege level to log into the device.

The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

Default Setting

Level 15

Command Mode

Normal Exec

Command Usage

- “super” is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the **enable password** command on page 4-21.)
- The “#” character is appended to the end of the prompt to indicate that the system is in privileged access mode.
- You only need to use Level 15. Setting the password for Level 0 has no effect.
- You cannot set a null password with the **enable password** command. You will have to enter a password to access the Privileged Exec mode.

Example

```
Console#enable
Console#
```

Related Commands

disable
enable password (4-21)

disable

Use this command to return to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See “Understanding Command Modes” on page 4-5.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The “>” character is appended to the end of the prompt to indicate that the system is in normal access mode.

 © 2004 Foundry Networks, Inc.

Example

```
Console#disable
Console>
```

Related Commands

enable (4-9)

configure

Use this command to activate Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, including Interface Configuration, Line Configuration, and VLAN Database Configuration. See “Understanding Command Modes” on page 4-5.

Syntax

configure [*terminal*]

- *terminal* - Specifies where the commands come in. Typing *terminal* is optional for compatibility with existing BigIron command line syntax.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#configure
Console(config)#
```

Related Commands

end (4-12)

show history

Use this command to show the contents of the command history buffer.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The history buffer size is fixed at 20 commands.

 © 2004 Foundry Networks, Inc.

Example

In this example, the show history command lists the contents of the command history buffer:

```
Console#show history
Exection command history:
 3 sh logging flash
 2 sh interfaces
 1 sh history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```
Console#!2
Console#config
Console(config)#
```

reload

Use this command to restart the system.

Note: When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the **copy running-config startup-config** command.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the switch:

```
Console#reload
System will be restarted, continue <y/n>? y
```


© 2004 Foundry Networks, Inc.

prompt

Use this command to customize the CLI prompt. Use the **no** form to revert to the default prompt.

Syntax

prompt *string*
no prompt

string - Any alphanumeric string to use for the command prompt. (Maximum length: 255 characters)

Default Setting

Console

Command Mode

Global Configuration

Example

```
Console(config)#prompt EIF2402CF
EIF2402CF(config)#
```

end

Use this command to return to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

exit

Use this command to return to the previous configuration mode or exit the configuration program.

Default Setting

None

Command Mode

Any

 © 2004 Foundry Networks, Inc.

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

quit

Use this command to exit the configuration program.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The quit and exit commands can both exit the configuration program.

Example

This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

Flash/File Commands

These commands are used to manage system code and configuration files.

Command	Function	Mode	Page
copy	Copies a code image or a switch configuration to or from flash memory or a TFTP server	PE	4-14
delete	Deletes a file or code image	PE	4-15
dir	Displays a list of files in flash memory	PE	4-16
whichboot	Displays the files booted	PE	4-16
boot system	Specifies the file or image used to start up the system	GC	4-17

© 2004 Foundry Networks, Inc.

copy

Use this command to move (upload/download) a code image or configuration file between the switch's flash memory and a TFTP server. When you save the system code or configuration settings to a file on a TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the TFTP server and the quality of the network connection.

Syntax

copy *file* {**file** | **running-config** | **startup-config** | **tftp**}
copy running-config {**file** | **startup-config** | **tftp**}
copy startup-config {**file** | **running-config** | **tftp**}
copy tftp {**file** | **running-config** | **startup-config** | **https-certificate**}

- *file* - Keyword that allows you to copy to/from a file.
- **running-config** - Keyword that allows you to copy to/from the current running configuration.
- **startup-config** - The configuration used for system initialization.
- **tftp** - Keyword that allows you to copy to/from a TFTP server.
- **https-certificate** - Copies an HTTPS certificate from an TFTP server to the switch.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The system prompts for data required to complete the copy command.
- File names are case-sensitive, should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- The number of user-defined configuration files is limited only by available flash memory space.
- You can use "Factory_Default_Config.cfg" as the source to copy from the factory default configuration file, but you cannot use "Factory_Default_Config.cfg" as the destination.
- To replace the startup configuration, you must use startup-config as the destination.
- The Boot ROM image cannot be uploaded or downloaded from the TFTP server. You must use a direct console connection and access the download menu during a boot up to download the Boot ROM (or diagnostic) image. See "Upgrading Firmware via the Serial Port" on page C-1 for more details.

Example

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
/
Console#
```

 © 2004 Foundry Networks, Inc.

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name : startup
/
Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
/
Console#
```

The following example shows how to copy a secure-site certificate from an TFTP server. It then reboots the switch to activate the certificate::

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: ********

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

delete

Use this command to delete a file or image.

Syntax

delete *filename*

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If the file type is used for system startup, then this file cannot be deleted.
- “Factory_Default_Config.cfg” cannot be deleted.

Example

This example shows how to delete the test2.cfg configuration file from flash memory.

```
Console#delete test2.cfg
Console#
```

Related Commands

dir (4-16)

© 2004 Foundry Networks, Inc.

dir

Use this command to display a list of files in flash memory.

Syntax

dir [**boot-rom** | **config** | **opcode** [:*filename*]]

The type of file or image to display includes:

- **boot-rom** - Boot ROM (or diagnostic) image file
- **config** - Switch configuration file
- **opcode** - Run-time operation code image file.
- *filename* - Name of the file or image. If this file exists but contains errors, information on this file cannot be shown.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If you enter the command **dir** without any parameters, the system displays all files.
- File information is shown below:

Column Heading	Description
file name	The name of the file.
file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
size	The length of the file in bytes.

Example

The following example shows how to display all file information:

```
Console#dir
                        file name      file type startup size (byte)
 --------------------------------- -------------- ------- -----------
              FoundryDiag2.0.2.4 Boot-Rom image       Y      816112
           FoundryRuntime2.2.4.11 Operation Code       Y     2213756
      Factory_Default_Config.cfg    Config File       N         374
                          set-ip    Config File       Y        2867
                         startup    Config File       Y        3847
 ------------------------------------------------------------------------
                                      Total free space:   4063232
Console#
```

whichboot

Use this command to display which files booted.

Default Setting

None

Command Mode

Privileged Exec

 © 2004 Foundry Networks, Inc.

Example

This example shows the information displayed by the **whichboot** command. See the table on the previous page for a description of the file information displayed by this command.

```
Console#whichboot
                        file name      file type startup size (byte)
 -------------------------------- -------------- ------- -----------
 Unit1:
              FoundryDiag2.0.2.4 Boot-Rom image       Y      816112
            FoundryRuntime2.2.4.11 Operation Code       Y     2213756
                           set-ip    Config File       Y        2867
Console#
```

boot system

Use this command to specify the file or image used to start up the system.

Syntax

boot system {**boot-rom**| **config** | **opcode**}: *filename*

The type of file or image to set as a default includes:

- **boot-rom** - Boot ROM
- **config** - Configuration file
- **opcode** - Run-time operation code

The colon (:) is required.

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- A colon (:) is required after the specified file type.
- If the file contains an error, it cannot be set as the default file.

Example

```
Console(config)#boot system config: startup
Console(config)#
```

Related Commands

dir (4-16)
whichboot (4-16)

© 2004 Foundry Networks, Inc.

System Management Commands

These commands are used to control system logs, passwords, user name, browser configuration options, and display or configure a variety of other system information.

Command	Function	Mode	Page
Device Description Command			
hostname	Specifies or modifies the host name for the device	GC	4-20
User Access Commands			
username	Sets user name authentication at login	GC	4-20
enable password	Sets a password to control access to various privilege levels	GC	4-21
IP Filter Commands			
management	Configures IP addresses that are allowed management access	GC	4-22
show management	Displays the client IP addresses that are allowed management access to the switch through various protocols.	PE	4-23
Time Commands			
calendar set	Set the system date and time	PE	4-55
show calendar	Display the current date and time setting	NE, PE	4-55
Jumbo Frame Command			
jumbo frame	Allows jumbo frames to pass through the switch	GC	4-23
Unit ID Command			
light unit	Displays the unit ID of a switch using its front-panel LED indicators	NE, PE	4-24
Web Server Commands			
ip http port	Specifies the port to be used by the Web browser interface	GC	4-24
ip http server	Allows the switch to be monitored or configured from a browser	GC	4-25
ip http secure-server	Enables the HTTPS server on the switch	GC	4-25
ip http secure-port	Specifies the UDP port number used for HTTPS connection to the switch's Web interface	GC	4-26
Secure Shell Commands			
ip ssh server	Enables the SSH 2.0 server on the switch	GC	4-35
calendar set	Sets the system clock	PE	4-55
ip ssh	Specifies the authentication timeout for the SSH server and the number of retries allowed by a client	GC	4-35
disconnect ssh	Terminates an SSH connection	PE	4-36
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE	4-37
show calendar	Displays the system clock	PE	4-55
ip ssh server	Enables the SSH server on the switch	GC	4-35

© 2004 Foundry Networks, Inc.

Command	Function	Mode	Page
ip ssh timeout	Specifies the authentication timeout for the SSH server	GC	4-29
ip ssh authentication-retries	Specifies the number of retries allowed by a client	GC	4-30
ip ssh server-key size	Sets the SSH server key size	GC	4-30
copy tftp public-key	Copies the user's public key from a TFTP server to the switch	PE	4-14
delete public-key	Deletes the public key for the specified user	PE	4-31
ip ssh crypto host-key generate	Generates the host key	PE	4-31
ip ssh crypto zeroize	Clear the host key from RAM	PE	4-32
ip ssh save host-key	Saves the host key from RAM to flash memory	PE	4-32
disconnect ssh	Terminates a line connection	PE	4-36
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE	4-33
show ssh	Displays the status of current SSH sessions	PE	4-36
show public-key	Shows the public key for the specified user or for the host	PE	4-34
show users	Shows SSH users, including privilege level and public key type	PE	4-47
Event Logging Commands			
logging on	Controls logging of error messages	GC	4-37
logging history	Limits syslog messages saved to memory based on severity	GC	4-38
logging host	Adds a syslog server host IP address that will receive logging messages	GC	4-39
logging facility	Sets the facility type for remote logging of syslog messages	GC	4-39
logging trap	Limits syslog messages saved to a remote server based on severity	GC	4-40
clear logging	Clears messages from the logging buffer	PE	4-41
show log	Displays the contents of the log buffer	PE	4-41
show logging	Displays the state of logging	PE	4-42
System Status Commands			
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE	4-43
show running-config	Displays the configuration data currently in use	PE	4-44
show system	Displays system information	NE, PE	4-46
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client	NE, PE	4-47
show version	Displays version information for the system	NE, PE	4-48

© 2004 Foundry Networks, Inc.

hostname

Use this command to specify or modify the host name for this device. Use the **no** form to restore the default host name.

Syntax

hostname *name*
no hostname

name - The name of this host. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#hostname EdgeIron 4802CF
Console(config)#
```

username

Use this command to require user name authentication at login. Use the **no** form to remove a user name.

Syntax

username *name* {**access-level** *level* | **nopassword** | **password** {**0** | **7**} *password***}**
no username *name*

- *name* - The name of the user.
  Up to 8 characters, case sensitive.
  Maximum number of users: 16
- **access-level** *level* - Specifies the user level.
- The device has two predefined privilege levels: **0**: Normal Exec, **15**: Privileged Exec.
- **nopassword** - No password is required for this user to log in.
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- **password** *password* - The authentication password for the user. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default access level is Normal Exec.
- The factory defaults for the user names and passwords are:

username	access-level	password
guest admin	0 15	guest admin

Command Mode

Global Configuration

© 2004 Foundry Networks, Inc.

Command Usage

The encrypted password is required for compatiblity with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

This example shows how the set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

enable password

After initially logging onto the system, you should set the administrator (Privileged Exec) and guest (Normal Exec) passwords. Remember to record them in a safe place. Use the enable password command to set the password for access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

Syntax

enable password [**level** *level*] {**0** | **7**} *password*
no enable password [**level** *level*]

- **level** *level* - Level for which the password applies.
- The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Only level 15 is valid for this command.
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- *password* - password for this privilege level.

Default Setting

This default password is “super”

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatiblity with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

enable (4-9)

© 2004 Foundry Networks, Inc.

management

This command specifies the client IP addresses that are allowed management access to the switch through various protocols. Use the **no** form to restore the default setting.

Syntax

[**no**] **management** {**all-client** | **http-client** | **snmp-client** | **telnet-client**} *start-address* [*end-address*]

- **all-client** - Adds IP address(es) to the SNMP, web and Telnet groups.
- http-client - Adds IP address(es) to the web group.
- snmp-client - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.
- start-address - A single IP address, or the starting address of a range.
- end-address - The end address of a range.

Default Setting

All addresses

Command Mode

Global Configuration

Command Usage

- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Example

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

 © 2004 Foundry Networks, Inc.

show management

This command displays the client IP addresses that are allowed management access to the switch through various protocols.

Syntax

show management {**all-client** | **http-client** | **snmp-client** | **telnet-client**}

- **all-client** - Adds IP address(es) to the SNMP, web and Telnet groups.
- http-client - Adds IP address(es) to the web group.
- snmp-client - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.

Command Mode

Global Configuration

Example

```
Console#show management all-client
Management Ip Filter
 Http-Client:
   Start ip address      End ip address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 Snmp-Client:
   Start ip address      End ip address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 Telnet-Client:
   Start ip address      End ip address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

Console#
```

jumbo frame

Use this command to enable jumbo frames through the switch. Use the **no** form to disable jumbo frames.

Syntax

jumbo frame
no jumbo frame

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 9000 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

© 2004 Foundry Networks, Inc.

- To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.
- Enabling jumbo frames will limit the maximum threshold for broadcast storm control to 64 packets per second. (See the “broadcast” command on page 4-114.)

Example

```
Console(config)#jumbo frame
Console(config)#
```

light unit

Use this command to display the unit ID of a switch using its front-panel LED indicators.

Syntax

light unit [*unit*]

- *unit* - specifies a unit in a switch stack to light the panel LEDs

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

- The unit ID is displayed using the port status LED indicators for ports 1 to 8. When the **light unit** command is entered, the LED corresponding to the switch’s ID will flash for about 15 seconds.

Note: This feature is only supported on the EdgeIron 2402CF.

Example

```
Console#light unit 1
Console#
```

ip http port

Use this command to specify the TCP port number used by the Web browser interface. Use the **no** form to use the default port.

Syntax

ip http port *port-number*
no ip http port

port-number - The TCP port to be used by the browser interface. (Range: 1-65535)

Default Setting

80

Command Mode

Global Configuration

 © 2004 Foundry Networks, Inc.

Example

```
Console(config)#ip http port 769
Console(config)#
```

Related Commands

ip http server

ip http server

Use this command to allow this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

ip http server
no ip http server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip http server
Console(config)#
```

Related Commands

ip http port (4-24)

ip http secure-server

Use this command to enable the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's Web interface. Use the **no** form to disable this function.

Syntax

ip http secure-server
no ip http secure-server

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- Both HTTP and HTTPS service can be enabled independently.
- If you enable HTTPS, you must indicate this in the URL: **https://***device*[*port_number*]

© 2004 Foundry Networks, Inc.

- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
  A padlock icon should appear in the status bar for Internet Explorer 5.x and Netscape Navigator 4.x.
- The following Web browsers and operating systems currently support HTTPS:

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000
Netscape Navigator 4.76 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Solaris 2.6

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands

ip http secure-port (4-26)
copy tftp https-certificate (4-14)

ip http secure-port

Use this command to specify the UDP port number used for HTTPS/SSL connection to the switch's Web interface. Use the **no** form to restore the default port.

Syntax

ip http secure-port *port_number*
no ip http secure-port

- *port_number* – The UDP port used for HTTPS/SSL. (Range: 1-65535)

Default Setting

443

Command Mode

Global Configuration

Command Usage

- You cannot configure the HTTP and HTTPS servers to use the same port.
- If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format:
  https://*device***:***port_number*

 © 2004 Foundry Networks, Inc.

Example

```
Console(config)#ip http secure-port 1000
Console(config)#
```

Related Commands

ip http secure-server (4-25)

Secure Shell Commands

The Berkley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rlogin* (remote login), *rsh* (remote shell), and *rcp* (remote copy), are not secure from hostile attacks.

The Secure Shell (SSH 2.0) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH 2.0 can also provide remote management access to this switch as a secure replacement for Telnet. When a client contacts the switch via the SSH protocol, the switch uses a public-key that the client must match along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

This section describes the commands used to configure the SSH 2.0 server. However, note that you also need to install a SSH client on the management station when using this protocol to configure the switch.

Note: The switch supports SSH Version 2.0.

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified by the **authentication login** command on page 4-57. If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch and enable the SSH 2.0 server.

 © 2004 Foundry Networks, Inc.

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – Use the **ip ssh crypto host-key generate** command to create a host public/private key pair.

2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

   10.1.0.54 1024 35 156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233765468017262725714134287629413011961955667825956641048695742788814620651941746772984865468615717739390164779355942303577413098022737087794545240839717526463580581767167095748047761117

3. Import Client's Public Key to the Switch – Use the **copy tftp public-key** command to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch with the username command as described on page 4-20.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example:

   1024 35 134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643 steve@192.168.1.19

4. Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. Enable SSH Service – Use the **ip ssh server** command to enable the SSH server on the switch.

6. Configure Challenge-Response Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can gain access. The following exchanges take place during this process:

   a. The client sends its public key to the switch.

   b. The switch compares the client's public key to those stored in memory.

   c. If a match is found, the switch uses the public key to encrypt a random sequence of bytes, and sends this string to the client.

   d. The client uses its private key to decrypt the bytes, and sends the decrypted bytes back to the switch.

   e. The switch compares the decrypted bytes to the original bytes it sent. If the two sets match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

 © 2004 Foundry Networks, Inc.

Note: To use SSH 2.0 with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

ip ssh server

Use this command to enable the Secure Shell (SSH 2.0) server on this switch. Use the **no** form to disable this service.

Syntax

ip ssh server
no ip ssh server

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- You must generate the host key before enabling the SSH 2.0 server.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

Related Commands

ip ssh crypto host-key generate (4-31)
show ssh (4-36)

ip ssh timeout

Use this command to configure the timeout for the SSH 2.0 server. Use the **no** form to restore the default setting.

Syntax

ip ssh timeout *seconds*
no ip ssh timeout

seconds – The timeout for client response during SSH negotiation. (Range: 1-120)

Default Setting

10 seconds

Command Mode

Global Configuration

 © 2004 Foundry Networks, Inc.

Command Usage

The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the **exec-timeout** command for vty sessions.

Example

```
Console(config)#ip ssh timeout 60
Console(config)#
```

Related Commands

exec-timeout (4-103)
show ip ssh (4-37)

ip ssh authentication-retries

Use this command to configure the number of times the SSH 2.0 server attempts to reauthenticate a user. Use the **no** form to restore the default setting.

Syntax

ip ssh authentication-retries *count*
no ip ssh authentication-retries

count – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default Setting

3

Command Mode

Global Configuration

Example

```
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

Related Commands

show ip ssh (4-37)

ip ssh server-key size

Use this command to set the SSH 2.0 server key size. Use the **no** form to restore the default setting.

Syntax

ip ssh server-key size *key-size*
no ip ssh server-key size

key-size – The size of server key. (Range: 512-896 bits)

Default Setting

768 bits

Command Mode

Global Configuration

 © 2004 Foundry Networks, Inc.

Command Usage

- The server key is a private key that is never shared outside the switch.
- The host key is shared with the SSH 2.0 client, and is fixed at 1024 bits.

Example

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

delete public-key

Use this command to delete the specified user's public key.

Syntax

delete public-key *username* [**dsa** | **rsa**]

- username – Name of an SSH user. (Range: 1-8 characters)
- **dsa** – DSA public key type.
- **rsa** – RSA public key type.

Default Setting

Deletes both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#delete public-key admin dsa
Console#
```

ip ssh crypto host-key generate

Use this command to generate the host key pair (i.e., public and private).

Syntax

ip ssh crypto host-key generate [**dsa** | **rsa**]

- **dsa** – DSA key type.
- **rsa** – RSA key type.

Default Setting

Generates both the DSA and RSA key pairs.

Command Mode

Privileged Exec

Command Usage

- This command stores the host key pair in memory (i.e., RAM). Use the **ip ssh save host-key** command to save the host key pair to flash memory.
- Some SSH 2.0 client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, you must manually create a known hosts file and place the host public key in it.
- The SSH 2.0 server uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

© 2004 Foundry Networks, Inc.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#
```

Related Commands

ip ssh crypto zeroize (4-32)
ip ssh save host-key (4-32)

ip ssh crypto zeroize

Use this command to clear the host key from memory (i.e. RAM).

Syntax

ip ssh crypto zeroize [**dsa** | **rsa**]

- **dsa** – DSA key type.
- **rsa** – RSA key type.

Default Setting

Clears both the DSA and RSA key.

Command Mode

Privileged Exec

Command Usage

- This command clears the host key from volatile memory (RAM). Use the **no ip ssh save host-key** command to clear the host key from flash memory.
- The SSH 2.0 server must be disabled before you can execute this command.

Example

```
Console#ip ssh crypto zeroize dsa
Console#
```

Related Commands

ip ssh crypto host-key generate (4-31)
ip ssh save host-key (4-32)
no ip ssh server (4-35)

ip ssh save host-key

Use this command to save host key from RAM to flash memory.

Syntax

ip ssh save host-key [**dsa** | **rsa**]

- **dsa** – DSA key type.
- **rsa** – RSA key type.

Default Setting

Saves both the DSA and RSA key.

Command Mode

Privileged Exec

 © 2004 Foundry Networks, Inc.

Example

```
Console#ip ssh save host-key dsa
Console#
```

Related Commands

ip ssh crypto host-key generate (4-31)

show ip ssh

Use this command to display the connection settings used when authenticating client access to the SSH 2.0 server.

Command Mode

Privileged Exec

Example

```
Console#show ip ssh
SSH Enabled - version 1.99
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#
```

show ssh

Use this command to display the current SSH 2.0 server connections.

Command Mode

Privileged Exec

Example

```
Console#show ssh
Connection  Version State            Username Encryption
0           2.0     Session-Started  admin    ctos aes128-cbc-hmac-md5
                                              stoc aes128-cbc-hmac-md5

Console#
```

Field	Description
Session	The session number. (Range: 0-3)
Version	The Secure Shell version number.
State	The authentication negotiation state. (Values: Negotiation-Started, Authentication-Started, Session-Started)
Username	The user name of the client.

© 2004 Foundry Networks, Inc.

Field	Description
Encryption	The encryption method is automatically negotiated between the client and server. Options for SSHv2.0 can include different algorithms for the client-to-server (ctos) and server-to-client (stoc): aes128-cbc-hmac-sha1 aes192-cbc-hmac-sha1 aes256-cbc-hmac-sha1 3des-cbc-hmac-sha1 blowfish-cbc-hmac-sha1 aes128-cbc-hmac-md5 aes192-cbc-hmac-md5 aes256-cbc-hmac-md5 3des-cbc-hmac-md5 blowfish-cbc-hmac-md5 Terminology: DES – Data Encryption Standard (56-bit key) 3DES – Triple-DES (Uses three iterations of DES, 112-bit key) aes – Advanced Encryption Standard (160 or 224-bit key) blowfish – Blowfish (32-448 bit key) cbc – cypher-block chaining sha1 – Secure Hash Algorithm 1 (160-bit hashes) md5 – Message Digest algorithm number 5 (128-bit hashes)

show public-key

Use this command to show the public key for the specified user or for the host.

Syntax

show public-key [**user** [*username*]| **host**]

username – Name of an SSH user. (Range: 1-8 characters)

Default Setting

Shows all public keys.

Command Mode

Privileged Exec

Command Usage

- If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.
- When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 35), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

© 2004 Foundry Networks, Inc.

Example

```
Console#show public-key host
Host:
RSA:
1024 35
156849954018676692593339467750546173253136748908365472541502024559319986854435836165199
992332979817660658309586108259132128902337654680172627257141342876294130119619555678259
566410486957427888146206519417467729848654686157177393901647793559423035774130980227370
708779454524083971752646358058176716709574804776117
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h2Hxc
YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfv
JlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdfQGNIjwbvwrNLaQ77isi
wAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMU01VFDly3IR
2G395NLy5Qd7ZDxfA9mCOfT/yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm
iFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOy
DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2
o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7 w0W
Console#
```

ip ssh

Use this command to configure authentication control parameters for the Secure Shell (SSH 2.0) server on this switch. Use the **no** form to restore the default settings.

Syntax

ip ssh {[**timeout** *seconds*] | [**authentication-retries** *count*]}
no ip ssh {[**timeout**] | [**authentication-retries**]}

- *seconds* – The timeout for client response during SSH negotiation. (Range: 1-120)
- *count* – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default Setting

timeout: 120 seconds
count: 3

Command Mode

Global Configuration

Command Usage

The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH 2.0 session has been established, the timeout for user input is controlled by the **exec-timeout** command for vty sessions.

Example

```
Console(config)#ip ssh timeout 60
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

Related Commands

show ip ssh (4-37)

ip ssh server

Use this command to enable the Secure Shell (SSH 2.0) server on this switch. Use the **no** form to disable this service.

Syntax

ip ssh server
no ip ssh server

 © 2004 Foundry Networks, Inc.

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The SSH 2.0 server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- The SSH 2.0 server uses RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

Example

```
Console(config)#ip ssh server
Console(config)#
```

Related Commands

show ssh (4-36)

disconnect ssh

Use this command to terminate a Secure Shell (SSH 2.0) client connection.

Syntax

disconnect ssh *connection-id*

connection-id – The session identifier as displayed in the **show ip ssh** command.

Command Mode

Privileged Exec

Example

```
Console#disconnect ssh 0
Console#
```

Related Commands

show ip ssh (4-37)

show ssh

Use this command to display the current Secure Shell (SSH 2.0) server connections.

Command Mode

Privileged Exec

Command Usage

This command shows the following information:

- **Session** – The session number. (Range: 0-3)
- **Username** – The user name of the client.
- **Version** – The Secure Shell version number.

 © 2004 Foundry Networks, Inc.

- **Encrypt method** – The encryption method. (Options: cipher-des, cipher-3des)
- **Negotiation state** – The authentication negotiation state.

Example

```
Console#show ssh
Information of secure shell
Session Username Version Encrypt method Negotiation state
------- -------- ------- -------------- -----------------
      0    admin   2.0      cipher-3des   session-started
Console#
```

show ip ssh

Use this command to display the connection settings used when authenticating client access to the Secure Shell (SSH 2.0) server.

Command Mode

Privileged Exec

Example

```
Console#show ip ssh
Information of secure shell
SSH status: enable
SSH authentication timeout: 120
SSH authentication retries: 3
Console#
```

Related Commands

ip ssh (4-35)

Event Logging Commands

The system can be configured to send debug and error messages to a logging process. This logging process controls the type of error messages that are stored in switch memory or sent to a remote syslog server.

logging on

Use this command to control logging of error messages. This command sends debug or error messages to a logging process. The **no** form disables the logging process.

Syntax

logging on
no logging on

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to switch memory or sent to remote syslog servers. You can use the **logging history** command to control the type of error messages that are stored in memory. The **logging trap** command controls the type of error messages that are sent to specified syslog servers.

 © 2004 Foundry Networks, Inc.

Example

```
Console(config)#logging on
Console(config)#
```

Related Commands

logging history
logging trap (4-40)
clear logging (4-41)

logging history

Use this command to limit syslog messages saved to switch memory based on severity. The **no** form returns the logging of syslog messages to the default level.

Syntax

logging history {**flash** | **ram**} *level*
no logging history {**flash** | **ram**}

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).
- *level* - One of the level arguments listed below. Messages sent include the selected level up through level 0.

Level Argument	Level*	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)	LOG_CRIT
errors	3	Error conditions (e.g., invalid input, default used)	LOG_ERR
warnings	4	Warning conditions (e.g., return false, unexpected return)	LOG_WARNING
notifications	5	Normal but significant condition, such as cold start	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

* There are only Level 2, 5 and 6 error messages for the current firmware release.

Default Setting

Flash: errors (level 3 - 0)
RAM: warnings (level 7 - 0)

Command Mode

Global Configuration

 © 2004 Foundry Networks, Inc.

Command Usage

The message level specified for flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.

Example

```
Console(config)#logging history ram 0
Console(config)#
```

logging host

Use this command to add a syslog server host IP address that will receive logging messages. Use the **no** form to remove a syslog server host.

Syntax

logging host *host_ip_address*
no logging host *host_ip_address*

host_ip_address - The IP address of a syslog server.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- By using this command more than once you can build up a list of host IP addresses.
- The maximum number of host IP addresses allowed is five.

Example

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

logging facility

Use this command to set the facility type for remote logging of syslog messages. Use the **no** form to return the type to the default.

Syntax

logging facility *type*
no logging facility *type*

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

Default Setting

23

Command Mode

Global Configuration

 © 2004 Foundry Networks, Inc.

Example

```
Console(config)#logging facility 19
Console(config)#
```

logging trap

Use this command to limit syslog messages saved to a remote server based on severity. Use the **no** form to return the remote logging of syslog messages to the default level.

Syntax

logging trap *level*
no logging trap *level*

level - One of the level arguments listed below. Messages sent include the selected level up through level 0.

Level Argument	Level*	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)	LOG_CRIT
errors	3	Error conditions (e.g., invalid input, default used)	LOG_ERR
warnings	4	Warning conditions (e.g., return false, unexpected return)	LOG_WARNING
notifications	5	Normal but significant condition, such as cold start	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

* There are only Level 2, 5 and 6 error messages for the current firmware release.

Default Setting

Level 3 - 0

Command Mode

Global Configuration

Example

```
Console(config)#logging trap 4
Console(config)#
```

 © 2004 Foundry Networks, Inc.

clear logging

Use this command to clear messages from the log buffer.

Syntax

clear logging [**flash** | **ram**]

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear logging
Console#
```

Related Commands

show logging (4-42)

show log

This command displays the system and event messages stored in memory.

Syntax

show log {**flash** | **ram**}

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command shows the system and event messages stored in memory, including the time stamp, message level, program module, function, and event number.

© 2004 Foundry Networks, Inc.

Example

The following example shows sample messages stored in RAM.

```
Console#show log ram
[5] 00:01:06 2001-01-01
   "STA root change notification."
   level: 6, module: 6, function: 1, and event no.: 1
[4] 00:01:00 2001-01-01
   "STA root change notification."
   level: 6, module: 6, function: 1, and event no.: 1
[3] 00:00:54 2001-01-01
   "STA root change notification."
   level: 6, module: 6, function: 1, and event no.: 1
[2] 00:00:50 2001-01-01
   "STA topology change notification."
   level: 6, module: 6, function: 1, and event no.: 1
[1] 00:00:48 2001-01-01
   "VLAN 1 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
Console#show log ram login
   "User(guest/Console) (0.0.0.0) (Dec 15 09:36:24 2003)"
   "User(admin/Console) (0.0.0.0) (Dec 15 09:36:01 2003)"#
```

show logging

Use this command to display the logging configuration for system and event messages.

Syntax

show logging {**sendmail** | **flash** | **ram** | **trap**}

- **sendmail** - Displays settings for the SMTP event handler.
- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).
- **trap** - Messages sent to remote syslog servers.

Default Setting

None

Command Mode

Privileged Exec

 © 2004 Foundry Networks, Inc.

Example

```
Console#show logging flash
Syslog logging: Disable
History logging in FLASH: level errors
Console#show logging trap
Syslog logging: Enable
REMOTELOG status: enable
REMOTELOG facility type: local use 3
REMOTELOG level type: Warning conditions
REMOTELOG server ip address: 10.1.0.3
REMOTELOG server ip address: 10.1.0.4
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
Console#show logging ram
Syslog logging: Enable
History logging in RAM: level debugging
[3] 0:0:41 1/1/1
   "VLAN 1 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[2] 0:0:41 1/1/1
   "STP topology change notification."
   level: 6, module: 6, function: 1, and event no.: 1
[1] 0:0:12 1/1/1
   "Unit 1, Port  5 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[0] 0:0:11 1/1/1
   "System coldStart notification."
   level: 6, module: 6, function: 1, and event no.: 1
Console#
```

System Status Commands

Use the system status commands to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

show startup-config

Use this command to display the configuration file stored in non-volatile memory that is used to start up the system.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the show running-config command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - SNMP community strings
  - Users (names and access levels)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface
  - IP address configured for VLANs
  - Spanning tree settings
  - Any configured settings for the console port and Telnet

 © 2004 Foundry Networks, Inc.

Example

```
Console#show startup-config
building startup-config, please wait.....
!
phymap 00-04-80-bd-47-4d
!
sntp server 0.0.0.0 0.0.0.0 0.0.0.0
!
snmp-server community private rw
snmp-server community public ro
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
!
vlan 1 by port
!
!
spanning-tree mst configuration
 mst 1 vlan 1
 mst 2 vlan 2
 mst 3 vlan 3
 mst 4 vlan 4

   .
   .
   .
   .

 mst 64 vlan 64
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1

   .
   .
   .
   .

interface ethernet 1/24
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
!
interface vlan 1
 ip address 10.1.0.1 255.255.255.0
!
!
!no map ip precedence
no map ip dscp
!
!
line console
!
!
line vty
!
!
end
Console#
```

Related Commands

show running-config (4-44)

show running-config

Use this command to display the configuration information currently in use.

Default Setting

None

Command Mode

Privileged Exec

 © 2004 Foundry Networks, Inc.

Command Usage

- Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - SNMP community strings
  - Users (names, access levels, and encrypted passwords)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface
  - IP address configured for VLANs
  - Spanning tree settings
  - Any configured settings for the console port and Telnet

 © 2004 Foundry Networks, Inc.

Example

```
Console#sh running-config
building running-config, please wait.....
!
phymap 00-04-80-bd-47-4d
!
sntp server 0.0.0.0 0.0.0.0 0.0.0.0
!
!
snmp-server community private rw
snmp-server community public ro
!
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
!
vlan 1 by port
!
!
!
!
!
spanning-tree mst configuration
 mst 1 vlan 1
 mst 2 vlan 2
 mst 3 vlan 3
 mst 4 vlan 4

   .
   .
   .
   .

 mst 64 vlan 64
!
spanning-tree mst configuration
!
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
!
interface ethernet 1/2
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
!
interface ethernet 1/3
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
!
interface ethernet 1/4
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
!
interface ethernet 1/5
 switchport allowed vlan add 1 untagged
 switchport native vlan 1

interface vlan 1
 ip address 10.3.4.51 255.255.255.0
!
no map ip precedence
no map ip dscp
!
.
.
end
Console#
```

Related Commands

show startup-config (4-43)

show system

Use this command to display system information.

Default Setting

None

 © 2004 Foundry Networks, Inc.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- For a description of the items shown by this command, refer to “Displaying System Information” on page 3-6.
- The POST results should all display “PASS.” If any POST test indicates “FAIL,” contact Technical Support for assistance.

Example

```
Console#sh system
System description: Foundry Networks EdgeIron 24G
System OID string: 1.3.6.1.4.1.1991.1.5.1.1.4.1.1
System information
 System Up time: 0 days, 3 hours, 50 minutes, and 33.39 seconds
 System Name            : fff
 System Location        : [NONE]
 System Contact         : [NONE]
 MAC address            : 00-04-80-BD-47-4D
 Web server             : enable
 Web server port        : 80
 Web secure server      : enable
 Web secure server port : 443
 POST result
UART LOOP BACK Test.........PASS
DRAM Test..................PASS
Timer Test.................PASS
PCI Device 1 Test..........PASS
PCI Device 2 Test..........PASS
Switch Int Loopback test.....PASS

Done All Pass.
Console#
```

show users

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The session used to execute this command is indicated by a “*” symbol next to the Line (i.e., session) index number.

Example

```
Console#sh users
 Username accounts:
  Username Privilege Public-Key
  -------- --------- ----------
     admin        15       None
     guest         0       None

 Online users
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
* 0   console    admin           0:00:00
  1     vty 0    admin           0:04:37      10.1.0.19

Console#
```

 © 2004 Foundry Networks, Inc.

show version

Use this command to display hardware and software version information for the system.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

See “Displaying Switch Hardware/Software Versions” on page 3-7 for detailed information on the items displayed by this command.

Example

```
Console#show version
Unit1
 Serial number          :A329025054
 Hardware version       :R01
 Number of ports        :24
 Main power status      :up
 Redundant power status :not present
Agent(master)
 Unit id                :1
 Loader version         :2.0.2.2
 Boot rom version       :2.0.2.4
 Operation code version :2.2.4.11
Console#
```

SMTP Alert Commands

Configures SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

Command	Function	Mode	Page
SMTP			
logging sendmail host	SMTP servers to receive alert messages	GC	4-48
logging sendmail level	Severity threshold used to trigger alert messages	GC	4-49
logging sendmail source-email	Email address used for “From” field of alert messages	GC	4-50
logging sendmail destination-email	Email recipients of alert messages	GC	4-50
logging sendmail	Enables SMTP event handling	GC	4-50
show logging sendmail	Displays SMTP event handler settings	NE, PE	4-51

logging sendmail host

This command specifies SMTP servers that will be sent alert messages. Use the **no** form to remove an SMTP server.

Syntax

[**no**] **logging sendmail host** *ip_address*

ip_address - IP address of an SMTP server that will be sent alert messages for event handling.

 © 2004 Foundry Networks, Inc.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- You can specify up to three SMTP servers for event handing. However, you must enter a separate command to specify each server.
- To send email alerts, the switch first opens a connection, sends all the email alerts waiting in the queue one by one, and finally closes the connection.
- To open a connection, the switch first selects the server that successfully sent mail during the last connection, or the first server configured by this command. If it fails to send mail, the switch selects the next server in the list and tries to send mail again. If it still fails, the system will repeat the process at a periodic interval. (A trap will be triggered if the switch cannot successfully open a connection.)

Example

```
Console(config)#logging sendmail host 192.168.1.19
Console(config)#
```

logging sendmail level

This command sets the severity threshold used to trigger alert messages.

Syntax

logging sendmail level level

level - One of the system message levels (page 4-38). Messages sent include the selected level down to level 0. (Range: 0-7; Default: 7)

Default Setting

Level 7

Command Mode

Global Configuration

Command Usage

The specified level indicates an event threshold. All events at this level or higher will be sent to the configured email recipients. (For example, using Level 7 will report all events from level 7 to level 0.)

Example

This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail level 3
Console(config)#
```


© 2004 Foundry Networks, Inc.

logging sendmail source-email

This command sets the email address used for the “From” field in alert messages.

Syntax

logging sendmail source-email email-address

email-address - The source email address used in alert messages. (Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

You may use an symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

Example

This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail source-email bill@this-company.com
Console(config)#
```

logging sendmail destination-email

This command specifies the email recipients of alert messages. Use the **no** form to remove a recipient.

Syntax

[**no**] **logging sendmail destination-email** email-address

email-address - The source email address used in alert messages. (Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

You can specify up to five recipients for alert messages. However, you must enter a separate command to specify each recipient.

Example

```
Console(config)#logging sendmail destination-email ted@this-company.com
Console(config)#
```

logging sendmail

This command enables SMTP event handling. Use the **no** form to disable this function.

Syntax

[**no**] **logging sendmail**

 © 2004 Foundry Networks, Inc.

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#logging sendmail
Console(config)#
```

show logging sendmail

This command displays the settings for the SMTP event handler.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show logging sendmail
SMTP servers
-------------------------------------------
Active SMTP server: 0.0.0.0

SMTP minimum severity level: 7

SMTP destination email addresses
-------------------------------------------
ted@this-company.com

SMTP source email address: bill@this-company.com

SMTP status: Enable

Console#
```

Time Commands

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP), or by using information broadcast by local time servers.

Command	Function	Mode	Page
SNTP			
sntp client	Accepts time from specified time servers	GC	4-52
sntp server	Specifies one or more time servers	GC	4-52
sntp poll	Sets the interval at which the client polls for time	GC	4-53
sntp broadcast client	Accepts time from any time broadcast server	GC	4-53
show sntp	Shows current SNTP configuration settings	NE, PE	4-54
clock timezone	Sets the time zone for the switch's internal clock	GC	4-54
calendar set	Set the system date and time	PE	4-55
show calendar	Display the current date and time setting	NE, PE	4-55

© 2004 Foundry Networks, Inc.

sntp client

This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the **sntp servers** command. Use the **no** form to disable SNTP client requests.

Syntax

[no] sntp client

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the **sntp servers** command. It issues time synchronization requests based on the interval set via the **sntp poll** command.
- The SNTP time query method is set to client mode when the first **sntp client** command is issued. However, if the **sntp broadcast client** command is issued, then the **no sntp broadcast client** command must be used to return the switch to SNTP client mode.

Example

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current time:  Dec 23 02:52:44 2002
Poll interval: 60
Current mode: unicast
Console#
```

Related Commands

sntp server (4-52)
sntp poll (4-53)
sntp broadcast client (4-53)
show sntp (4-54)

sntp server

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list.

Syntax

sntp server [***ip1*** [***ip2*** [*ip3*]]]

ip - IP address of an time server (NTP or SNTP).

(Range: 1 - 3 addresses)

Default Setting

None

 © 2004 Foundry Networks, Inc.

Command Mode

Global Configuration

Command Usage

This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the **sntp poll** command.

Example

```
Console(config)#sntp server 10.1.0.19
Console#
```

Related Commands

sntp client (4-52)
sntp poll (4-53)
show sntp (4-54)

sntp poll

This command sets the interval between sending time requests when the switch is set to SNTP client mode. Use the **no** form to restore to the default.

Syntax

sntp poll *seconds*

no sntp poll

seconds - Interval between time requests. (Range: 16-16384 seconds)

Default Setting

16 seconds

Command Mode

Global Configuration

Command Usage

This command is only applicable when the switch is set to SNTP client mode.

Example

```
Console(config)#sntp poll 60
Console#
```

Related Commands

sntp client (4-52)

sntp broadcast client

This command synchronizes the switch's clock based on time broadcast from time servers (using the multicast address 224.0.1.1). Use the **no** form to disable SNTP broadcast client mode.

Syntax

[**no**] **sntp broadcast client**

© 2004 Foundry Networks, Inc.

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#sntp broadcast client
Console#
```

show sntp

This command displays the current time and configuration settings for the SNTP client, and indicates whether or not the local time has been properly updated.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the current time, the poll interval used for sending time synchronization requests (when the switch is set to SNTP client mode), and the current SNTP mode (i.e., client or broadcast).

Example

```
Console#show sntp
Current time:  Dec 23 05:13:28 2002
Poll interval: 16
Current mode:  unicast
Console#
```

clock timezone

This command sets the time zone for the switch's internal clock.

Syntax

clock timezone *name* **hour** *hours* **minute** *minutes* {**before-utc** | **after-utc**}

- *name* - Name of timezone, usually an acronym. (Range: 1-29 characters)
- *hours* - Number of hours before/after UTC. (Range: 1-12 hours)
- *minutes* - Number of minutes before/after UTC. (Range: 0-59 minutes)
- **before-utc** - Sets the local time zone before (east) of UTC.
- **after-utc** - Sets the local time zone after (west) of UTC.

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

 © 2004 Foundry Networks, Inc.

Example

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

Related Commands

show sntp (4-54)

calendar set

This command sets the system clock. It may be used if there is no time server on your network, or if you have not configured the switch to receive signals from a time server.

Syntax

calendar set *hour min sec* {day *month year* | *month day year*}

- *hour* - Hour in 24-hour format. (Range: 0 - 23)
- *min* - Minute. (Range: 0 - 59)
- *sec* - Second. (Range: 0 - 59)
- *month* - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**
- *day* - Day of month. (Range: 1 - 31)
- *year* - Year (4-digit). (Range: 2001 - 2101)

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows how to set the system clock to 15:12:34, February 1st, 2002.

```
Console#calendar set 15 12 34 February 31 2004
Console#
```

show calendar

This command displays the system clock.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show calendar set
15 12 34 February 31 2004
Console#
```


© 2004 Foundry Networks, Inc.

Authentication Commands

You can configure the switch to authenticate users logging into the system for management access using local or authentication-server methods. You can also enable port-based authentication for network client access using IEEE 802.1x.

Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS+-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to a switch.

The switch supports IEEE 802.1x (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first enter a user ID and password for authentication. Client authentication is controlled centrally by a RADIUS server using EAPOL (Extensible Authentication Protocol Over LANs).

Command	Function	Mode	Page
Authentication Method			
authentication login	Defines logon authentication method and precedence	GC	4-57
authentication enable	Defines the authentication method and precedence for command mode change	GC	4-58
RADIUS Client			
radius-server host	Specifies the RADIUS server	GC	4-58
radius-server port	Sets the RADIUS server network port	GC	4-59
radius-server key	Sets the RADIUS encryption key	GC	4-59
radius-server retransmit	Sets the number of retries	GC	4-60
radius-server timeout	Sets the interval between sending authentication requests	GC	4-60
show radius-server	Shows the current RADIUS settings	PE	4-60
TACACS+ Client			
tacacs-server host	Specifies the TACACS+ server	GC	4-61
tacacs-server port	Specifies the TACACS+ server network port	GC	4-61
tacacs-server key	Sets the TACACS+ encryption key	GC	4-62
show tacacs-server	Shows the current TACACS+ settings	GC	4-62
802.1x Port Authentication			
authentication dot1x default	Sets the default authentication server type	GC	4-62
dot1x default	Resets all dot1x parameters to their default values	GC	4-63
dot1x max-req	Sets the maximum number of times the switch will attempt to send a request to the client before authentication fails	GC	4-63
dot1x port-control	Sets dot1x mode for a port interface	IC	4-63
dot1x re-authenticate	Forces re-authentication on specific ports	PE	4-64

© 2004 Foundry Networks, Inc.

Command	Function	Mode	Page
dot1x re-authentication	Enables re-authentication for all ports	GC	4-64
dot1x timeout quiet-period	Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client	GC	4-64
dot1x timeout re-authperiod	Sets the time period after which a connected client must be re-authenticated	GC	4-65
dot1x timeout tx-period	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet	GC	4-65
show dot1x	Shows all dot1x related information	PE	4-66

authentication login

Use this command to define the login authentication method and precedence. Use the **no** form to restore the default.

Syntax

authentication login {[**local**] [**radius**] [**tacacs**]}
no authentication login

- **local** - Use local authentication.
- **radius** - Use RADIUS server authentication.
- **tacacs** - Use TACACS+ server authentication.

Default Setting

Local only

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server.
- RADIUS and TACACS+ logon authentication can control management access via the console port, a Web browser, or Telnet. These access options must be configured on the authentication server.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication login radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication login radius local
Console(config)#
```


© 2004 Foundry Networks, Inc.

Related Commands

username - for setting local user names and passwords (4-20)

authentication enable

This command defines the authentication method and precedence to use when changing from Exec command mode to Privileged Exec command mode with the **enable** command (see page 4-9). Use the **no** form to restore the default.

Syntax

authentication enable {[**local**] [**radius**] [**tacacs**]}
no authentication enable

- **local** - Use local password only.
- **radius** - Use RADIUS server password only.
- **tacacs** - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication enable radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication enable radius
Console(config)#
```

Related Commands

enable password - (4-21)

radius-server host

Use this command to specify the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server host *host_ip_address*
no radius-server host

host_ip_address - IP address of a RADIUS server.

 © 2004 Foundry Networks, Inc.

Default Setting

10.1.0.1

Command Mode

Global Configuration

Example

```
Console(config)#radius-server host 192.168.1.25
Console(config)#
```

radius-server port

Use this command to set the RADIUS server network port. Use the **no** form to restore the default.

Syntax

radius-server port *port_number*
no radius-server port

port_number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
Console(config)#radius-server port 181
Console(config)#
```

radius-server key

Use this command to set the RADIUS encryption key. Use the **no** form to restore the default.

Syntax

radius-server key *key_string*
no radius-server key

key_string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server key green
Console(config)#
```


© 2004 Foundry Networks, Inc.

radius-server retransmit

Use this command to set the number of retries. Use the **no** form to restore the default.

Syntax

radius-server retransmit *number_of_retries*
no radius-server retransmit

number_of_retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout

Use this command to set the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server timeout *number_of_seconds*
no radius-server timeout

number_of_seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

Use this command to display the current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

 © 2004 Foundry Networks, Inc.

Example

```
Console#show radius-server
Server IP address: 10.1.0.99
 Communication key with radius server:
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5
Console#
```

tacacs-server host

Use this command to specify the TACACS+ server. Use the **no** form to restore the default.

Syntax

tacacs-server host *host_ip_address*
no tacacs-server host

host_ip_address - IP address of a TACACS+ server.

Default Setting

10.11.12.13

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

tacacs-server port

Use this command to specify the TACACS+ server network port. Use the **no** form to restore the default.

Syntax

tacacs-server port *port_number*
no tacacs-server port

port_number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server port 181
Console(config)#
```


© 2004 Foundry Networks, Inc.

tacacs-server key

Use this command to set the TACACS+ encryption key. Use the **no** form to restore the default.

Syntax

tacacs-server key *key_string*
no tacacs-server key

key_string - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string.
(Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server key green
Console(config)#
```

show tacacs-server

Use this command to display the current settings for the TACACS+ server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show tacacs-server
Remote TACACS server configuration:
 Server IP address: 10.11.12.13
 Communication key with TACACS server:
 Server port number: 49
Console#
```

authentication dot1x default

Sets the default authentication server type. Use the **no** form to restore the default.

Syntax

authentication dot1x default radius
no authentication dot1x

Default Setting

RADIUS

Command Mode

Global Configuration

 © 2004 Foundry Networks, Inc.

Example

```
Console(config)#authentication dot1x default radius
Console(config)#
```

dot1x default

Sets all configurable dot1x global and port settings to their default values.

Command Mode

Global Configuration

Example

```
Console(config)#dot1x default
Console(config)#
```

dot1x max-req

Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. Use the **no** form to restore the default.

Syntax

dot1x max-req *count*
no dot1x max-req

count – The maximum number of requests (Range: 1-10)

Default

2 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x max-req 2
Console(config)#
```

dot1x port-control

Sets the dot1x mode on a port interface. Use the **no** form to restore the default.

Syntax

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}
no dot1x port-control

- **auto** – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.
- **force-authorized** – Configures the port to grant access to all clients, either dot1x-aware or otherwise.
- **force-unauthorized** – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

Default

force-authorized

© 2004 Foundry Networks, Inc.

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

dot1x re-authenticate

Forces re-authentication on all ports or a specific interface.

Syntax

dot1x re-authenticate [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.

Command Mode

Privileged Exec

Example

```
Console#dot1x re-authenticate
Console#
```

dot1x re-authentication

Enables periodic re-authentication globally for all ports. Use the **no** form to disable re-authentication.

Syntax

dot1x re-authentication
no dot1x re-authentication

Command Mode

Global Configuration

Example

```
Console(config)#dot1x re-authentication
Console(config)#
```

dot1x timeout quiet-period

Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. Use the **no** form of this command to reset the default.

Syntax

dot1x timeout quiet-period *seconds*
no dot1x timeout quiet-period *seconds*

seconds - The number of seconds. (Range: 1-65535)

Default

60 seconds

 © 2004 Foundry Networks, Inc.

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout quiet-period 350
Console(config)#
```

dot1x timeout re-authperiod

Sets the time period after which a connected client must be re-authenticated.

Syntax

dot1x timeout re-authperiod *seconds*
no dot1x timeout re-authperiod

seconds - The number of seconds. (Range: 1-65535)

Default

3600 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout re-authperiod 300
Console(config)#
```

dot1x timeout tx-period

Sets the time that the switch waits during an authentication session before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

Syntax

dot1x timeout tx-period *seconds*
no dot1x timeout tx-period

seconds - The number of seconds. (Range: 1-65535)

Default

30 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout tx-period 300
Console(config)#
```


© 2004 Foundry Networks, Inc.

show dot1x

Use this command to show general port authentication related settings on the switch or a specific interface.

Syntax

show dot1x [**statistics**] [**interface** *interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.

Command Mode

Privileged Exec

Command Usage

This command displays the following information:

- *Global 802.1X Parameters* – Displays the global port access control parameters that can be configured for this switch as described in the preceding pages, including reauth-enabled (page 4-64), reauth-period (page 4-65), quiet-period (page 4-64), tx-period (page 4-65), and max-req (page 4-63). It also displays the following global parameters which are set to a fixed value, including the following items:
  - supp-timeout – Supplicant timeout.
  - server-timeout – Server timeout.
  - reauth-max – Maximum number of reauthentication attempts.
- *802.1X Port Summary* – Displays the port access control parameters for each interface, including the following items:
  - Status – Administrative state for port access control.
  - Mode – Dot1x port control mode (page 4-63).
  - Authorized – Authorization status (yes or n/a - not authorized).
- *802.1X Port Details* – Displays detailed port access control settings for each interface as described in the preceding pages, including administrative status for port access control, Max request (page 4-63), Quiet period (page 4-64), Reauth period (page 4-65), Tx period (page 4-65), and Port-control (page 4-63). It also displays the following information:
  - Status – Authorization status (authorized or unauthorized).
  - Supplicant – MAC address of authorized client.
- *Authenticator State Machine*
  - State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
  - Reauth Count – Number of times connecting state is re-entered.
- *Backend State Machine*
  - State – Current state (including request, response, success, fail, timeout, idle, initialize).
  - Request Count – Number of EAP Request packets sent to the Supplicant without receiving a response.
  - Identifier(Server) – Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.

 © 2004 Foundry Networks, Inc.

- *Reauthentication State Machine*
  - State – Current state (including initialize, reauthenticate).

Example

```
Console#show dot1x
Global 802.1X Parameters
 reauth-enabled: yes
 reauth-period:  300
 quiet-period:   350
 tx-period:      300
 supp-timeout:   30
 server-timeout: 30
 reauth-max:     2
 max-req:        2

802.1X Port Summary
 Port Name     Status     Operation Mode                Mode     Authorized
       1/1   disabled        Single-Host      ForceAuthorized            n/a
       1/2   disabled        Single-Host      ForceAuthorized
.
.

       1/23   disabled        Single-Host     ForceAuthorized            yes
       1/24   disabled        Single-Host     ForceAuthorized

802.1X Port Details

802.1X is disabled on port 1
.
.
.

802.1X is enabled on port 26

Console#
```

Access Control List Commands

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code) or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, specify a mask to modify the precedence in which the rules are checked, and then bind the list to a specific port.

Access Control Lists

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped; and if no rules match for a list of all deny rules, the packet is accepted.

Note: The EdgeIron 2402CF and 4802CF do not support ACLs, but do support IP Management filtering.

© 2004 Foundry Networks, Inc.

There are three filtering modes:

- Standard IP ACL mode (STD-ACL) filters packets based on the source IP address.
- Extended IP ACL mode (EXT-ACL) filters packets based on source or destination IP address, as well as protocol type and protocol port number. If the TCP protocol is specified, then you can also filter packets based on the TCP control code.
- MAC ACL mode (MAC-ACL) filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

The following restrictions apply to ACLs:

- This switch supports ACLs for both ingress and egress filtering. However, you can only bind one IP ACL and one MAC ACL to any port for ingress filtering, and one IP ACL and one MAC ACL to any port for egress filtering. In other words, only four ACLs can be bound to an interface – Ingress IP ACL, Egress IP ACL, Ingress MAC ACL and Egress MAC ACL.
- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.
- Each ACL can have up to 32 rules.
- The maximum number of ACLs is also 32.
- However, due to resource restrictions, the average number of rules bound the ports should not exceed 20.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
- The switch does not support the explicit “deny any any” rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.
- Egress MAC ACLs only work for destination-mac-known packets, not for multicast, broadcast, or destination-mac-unknown packets.

The order in which active ACLs are checked is as follows:

1. User-defined rules in the Egress MAC ACL for egress ports.
2. User-defined rules in the Egress IP ACL for egress ports.
3. User-defined rules in the Ingress MAC ACL for ingress ports.
4. User-defined rules in the Ingress IP ACL for ingress ports.
5. Explicit default rule (permit any any) in the ingress IP ACL for ingress ports.
6. Explicit default rule (permit any any) in the ingress MAC ACL for ingress ports.
7. If no explicit rule is matched, the implicit default is permit all.

 © 2004 Foundry Networks, Inc.

Masks for Access Control Lists

You can specify optional masks that control the order in which ACL rules are checked. The switch includes two system default masks that pass/filter packets matching the permit/deny the rules specified in an ingress ACL. You can also configure up to seven user-defined masks for an ACL. A mask must be bound exclusively to one of the basic ACL types (i.e., Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL), but a mask can be bound to up to four ACLs of the same type.

Command Groups	Function	Page
IP ACLs	Configures ACLs based on IP addresses, TCP/UDP port number, protocol type, and TCP control code	4-69
MAC ACLs	Configures ACLs based on hardware addresses, packet format, and Ethernet type	4-80
ACL Information	Displays ACLs and associated rules; shows ACLs assigned to each port	4-90

IP ACLs

Command	Function	Mode	Page
access-list ip	Creates an IP ACL and enters configuration mode	GC	4-70
permit, deny	Filters packets matching a specified source IP address	STD-ACL	4-70
permit, deny	Filters packets meeting the specified criteria, including source and destination IP address, TCP/UDP port number, protocol type, and TCP control code	EXT-ACL	4-71
show ip access-list	Displays the rules for configured IP ACLs	PE	4-73
access-list ip mask-precedence	Changes to the mode for configuring access control masks	GC	4-73
mask	Sets a precedence mask for the ACL rules	IP-Mask	4-74
show access-list ip mask-precedence	Shows the ingress or egress rule masks for IP ACLs	PE	4-76
ip access-group	Adds a port to an IP ACL	IC	4-77
show ip access-group	Shows port assignments for IP ACLs	PE	4-77
map access-list ip	Sets the CoS value and corresponding output queue for packets matching an ACL rule	IC	4-78
show map access-list ip	Shows CoS value mapped to an access list for an interface	PE	4-79
match access-list ip	Changes the 802.1p priority, IP Precedence, or DSCP Priority of a frame matching the defined rule (i.e., also called packet marking)	IC	4-79
show marking	Displays the current configuration for packet marking	PE	4-80

© 2004 Foundry Networks, Inc.

access-list ip

This command adds an IP access list and enters configuration mode for standard or extended IP ACLs. Use the **no** form to remove the specified ACL.

Syntax

[**no**] **access-list ip** {**standard** | **extended**} *acl_name*

- **standard** – Specifies an ACL that filters packets based on the source IP address.
- **extended** – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- An egress ACL must contain all deny rules.
- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

Related Commands

permit, deny 4-70
ip access-group (4-77)
show ip access-list (4-73)

permit, deny (Standard ACL)

This command adds a rule to a Standard IP ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit** | **deny**} {**any** | *source bitmask* | **host** ***source***}

- **any** – Any source IP address.
- *source* – Source IP address.
- *bitmask* – Decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.

Default Setting

None

 © 2004 Foundry Networks, Inc.

Command Mode

Standard ACL

Command Usage

- New rules are appended to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Example

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Related Commands

access-list ip (4-70)

permit, **deny** (Extended ACL)

This command adds a rule to an Extended IP ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit** | **deny**} [*protocol-number* / **udp**]
{**any** | *source address-bitmask* / **host** *source*}
{**any** | *destination address-bitmask* / **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]] [**destination-port** *dport* [*port-bitmask*]]

[**no**] {**permit** | **deny**} **tcp**
{**any** | *source address-bitmask* / **host** *source*}
{**any** | *destination address-bitmask* / **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]] [**destination-port** *dport* [*port-bitmask*]]
[**control-flag** *control-flags flag-bitmask*]

- *protocol-number* – A specific protocol number. (Range: 0-255)
- *source* – Source IP address.
- *destination* – Destination IP address.
- *address-bitmask* – Decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.
- precedence – IP precedence level. (Range: 0-7)
- tos – Type of Service level. (Range: 0-15)
- *dscp* – DSCP priority level. (Range: 0-64)
- *sport* – Protocol* source port number. (Range: 0-65535)
- *dport* – Protocol* destination port number. (Range: 0-65535)
- *port-bitmask* – Decimal number representing the port bits to match. (Range: 0-65535)

 © 2004 Foundry Networks, Inc.

- *control-flags* – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- *flag-bitmask* – Decimal number representing the code bits to match.

* Includes TCP, UDP or other protocol types.

Default Setting

None

Command Mode

Extended ACL

Command Usage

- All new rules are appended to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- You can specify both Precedence and ToS in the same rule. However, if DSCP is used, then neither Precedence nor ToS can be specified.
- The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:
  - 1 (fin) – Finish
  - 2 (syn) – Synchronize
  - 4 (rst) – Reset
  - 8 (psh) – Push
  - 16 (ack) – Acknowledgement
  - 32 (urg) – Urgent pointer
- For example, use the code value and mask below to catch packets with the following flags set:
  - SYN flag valid, use “control-code 2 2”
  - Both SYN and ACK valid, use “control-code 18 18”
  - SYN valid and ACK invalid, use “control-code 2 18”

Example

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any dport 80
Console(config-ext-acl)#
```

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to “SYN.”

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any tcp control-code 2 2
Console(config-ext-acl)#
```

 © 2004 Foundry Networks, Inc.

Related Commands

access-list ip (4-70)

show ip access-list

This command displays the rules for configured IP ACLs.

Syntax

show ip access-list {**standard** | **extended**} [*acl_name*]

- **standard** – Specifies a standard IP ACL.
- **extended** – Specifies an extended IP ACL.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show ip access-list standard
IP standard access-list david:
  permit 10.7.1.1 255.255.255.0 any
  permit 192.168.1.0 255.255.255.0 any dport 80
  permit 192.168.1.0 255.255.255.0 any tcp control-code 2 2
Console#
```

Related Commands

permit, deny 4-70
ip access-group (4-77)

access-list ip mask-precedence

This command changes to the IP Mask mode used to configure access control masks. Use the **no** form to delete the mask table.

Syntax

[**no**] **access-list ip mask-precedence** {**in** | **out**}

- **in** – Ingress mask for ingress ACLs.
- **out** – Egress mask for egress ACLs.

Default Setting

Default system mask: Filter inbound packets according to specified IP ACLs.

Command Mode

Global Configuration

Command Usage

- A mask can only be used by all ingress ACLs or all egress ACLs.
- The precedence of the ACL rules applied to a packet is not determined by order of the rules, but instead by the order of the masks; i.e., the first mask that matches a rule will determine the rule that is applied to a packet.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.

© 2004 Foundry Networks, Inc.

Example

```
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#
```

Related Commands

mask (IP ACL) (4-74)
ip access-group (4-77)

mask (IP ACL)

This command defines a mask for IP ACLs. This mask defines the fields to check in the IP header. Use the **no** form to remove a mask.

Syntax

[**no**] **mask** [**protocol**]
{**any** | **host** | *source-bitmask*}
{**any** | **host** | *destination-bitmask*}
[**precedence**] [**tos**] [**dscp**]
[**source-port** [*port-bitmask*]] [**destination-port** [*port-bitmask]*]
[**control-flag** [*flag-bitmask*]]

- **protocol** – Check the protocol field.
- **any** – Any address will be matched.
- **host** – The address must be for a host device, not a subnetwork.
- *source-bitmask* – Source address of rule must match this bitmask.
- destination-bitmask – Destination address of rule must match this bitmask.
- precedence – Check the IP precedence field.
- **tos** – Check the TOS field.
- dscp – Check the DSCP field.
- source-port – Check the protocol source port field.
- destination-port – Check the protocol destination port field.
- port-bitmask – Protocol port of rule must match this bitmask. (Range: 0-65535)
- control-flag – Check the field for control flags.
- *flag-bitmask* – Control flags of rule must match this bitmask. (Range: 0-63)

Default Setting

None

Command Mode

IP Mask

Command Usage

- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules were entered.
- First create the required ACLs and ingress or egress masks before mapping an ACL to an interface.
- If you enter **dscp**, you cannot enter **tos** or **precedence**. You can enter both **tos** and **precedence** without **dscp**.

 © 2004 Foundry Networks, Inc.

- Masks that include an entry for a Layer 4 protocol source port or destination port can only be applied to packets with a header length of exactly five bytes.

Example

This example creates an IP ingress mask with two rules. Each rule is checked in order of precedence to look for a match in the ACL entries. The first entry matching a mask is applied to the inbound packet.

```
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

This shows that the entries in the mask override the precedence in which the rules are entered into the ACL. In the following example, packets with the source address 10.1.1.1 are dropped because the “deny 10.1.1.1 255.255.255.255” rule has the higher precedence according the “mask host any” entry.

```
Console(config)#access-list ip standard A2
Console(config-std-acl)#permit 10.1.1.0 255.255.255.0
Console(config-std-acl)#deny 10.1.1.1 255.255.255.255
Console(config-std-acl)#exit
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

This shows how to create a standard ACL with an ingress mask to deny access to the IP host 171.69.198.102, and permit access to any others.

```
Console(config)#access-list ip standard A2
Console(config-std-acl)#permit any
Console(config-std-acl)#deny host 171.69.198.102
Console(config-std-acl)#end
Console#show access-list
IP standard access-list A2:
  deny host 171.69.198.102
  permit any
Console#configure
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#exit
Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group A2 in
Console(config-if)#end
Console#show access-list
IP standard access-list A2:
  deny host 171.69.198.102
  permit any
Console#
```


© 2004 Foundry Networks, Inc.

This shows how to create an extended ACL with an egress mask to drop packets leaving network 171.69.198.0 when the Layer 4 source port is 23.

```
Console(config)#access-list ip extended A3
Console(config-ext-acl)#deny host 171.69.198.5 any
Console(config-ext-acl)#deny 171.69.198.0 255.255.255.0 any source-
   port 23
Console(config-ext-acl)#end
Console#show access-list
IP extended access-list A3:
  deny host 171.69.198.5 any
  deny 171.69.198.0 255.255.255.0 any source-port 23
Console#config
Console(config)#access-list ip mask-precedence out
Console(config-ip-mask-acl)#mask 255.255.255.0 any source-port
Console(config-ip-mask-acl)#exit
Console(config)#interface ethernet 1/15
Console(config-if)#ip access-group A3 out
Console(config-if)#end
Console#show access-list
IP extended access-list A3:
  deny 171.69.198.0 255.255.255.0 any source-port 23
  deny host 171.69.198.5 any
IP egress mask ACL:
  mask 255.255.255.0 any source-port
Console#
```

This is a more comprehensive example. It denies any TCP packets in which the SYN bit is ON, and permits all other packets. It then sets the ingress mask to check the deny rule first, and finally binds port 1 to this ACL. Note that once the ACL is bound to an interface (i.e., the ACL is active), the order in which the rules are displayed is determined by the associated mask.

```
Switch(config)#access-list ip extended 6
Switch(config-ext-acl)#permit any any
Switch(config-ext-acl)#deny tcp any any control-flag 2 2
Switch(config-ext-acl)#end
Console#show access-list
IP extended access-list A6:
  permit any any
  deny tcp any any control-flag 2 2
Console#configure
Switch(config)#access-list ip mask-precedence in
Switch(config-ip-mask-acl)#mask protocol any any control-flag 2
Switch(config-ip-mask-acl)#end
Console#sh access-list
IP extended access-list A6:
  permit any any
  deny tcp any any control-flag 2 2
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#configure
Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group A6 in
Console(config-if)#end
Console#show access-list
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#
```

show access-list ip mask-precedence

This command shows the ingress or egress rule masks for IP ACLs.

Syntax

show access-list ip mask-precedence [**in** | **out**]

- **in** – Ingress mask precedence for ingress ACLs.
- **out** – Egress mask precedence for egress ACLs.

Command Mode

Privileged Exec

 © 2004 Foundry Networks, Inc.

Example

```
Console#show access-list ip mask-precedence
IP ingress mask ACL:
  mask host any
  mask 255.255.255.0 any
Console#
```

Related Commands

mask (IP ACL) (4-74)

ip access-group

This command binds a port to an IP ACL. Use the **no** form to remove the port.

Syntax

[**no**] **ip access-group** *acl_name* {**in** | **out**}

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- **in** – Indicates that this list applies to ingress packets.
- **out** – Indicates that this list applies to egress packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.
- You must configure a mask for an ACL rule before you can bind it to a port.

Example

```
Console(config)#int eth 1/25
Console(config-if)#ip access-group standard david in
Console(config-if)#
```

Related Commands

show ip access-list (4-73)

show ip access-group

This command shows the ports assigned to IP ACLs.

Command Mode

Privileged Exec

Example

```
Console#show ip access-group
Interface ethernet 1/25
 IP standard access-list david
Console#
```

Related Commands

ip access-group (4-77)

© 2004 Foundry Networks, Inc.

map access-list ip

This command sets the output queue for packets matching an ACL rule. The specified CoS value is only used to map the matching packet to an output queue; it is not written to the packet itself. Use the **no** form to remove the CoS mapping.

Syntax

[**no**] **map access-list ip** *acl_name* **cos** *cos-value*

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- *cos-value* – CoS value. (Range: 0-7)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- You must configure an ACL mask before you can map CoS values to the rule.
- A packet matching a rule within the specified ACL is mapped to one of the output queues as shown in the following table. For information on mapping the CoS values to output queues, see **queue cos-map** on page 4-167.

EdgeIron 24G-A, 48G								
Priority	1	2	4	6	8	10	12	14
Queue	0	1	2	3	4	5	6	7

EdgeIron 4802CF, 2402CF				
Priority	1	4	16	64
Queue	0	1	2	3

EdgeIron 24G				
Priority	16	64	128	240
Queue	0	1	2	3

Example

```
Console(config)#interface ethernet 1/25
Console(config-if)#map access-list ip bill cos 0
Console(config-if)#
```

Related Commands

queue cos-map (4-167)
show map access-list ip (4-79)

© 2004 Foundry Networks, Inc.

show map access-list ip

This command shows the CoS value mapped to an IP ACL for the current interface. (The CoS value determines the output queue for packets matching an ACL rule.)

Syntax

show map access-list ip [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.

Command Mode

Privileged Exec

Example

```
Console#show map access-list ip
Access-list to COS of Eth 1/24
 Access-list ALS1 cos 0
Console#
```

Related Commands

map access-list ip (4-78)

match access-list ip

This command changes the IEEE 802.1p priority, IP Precedence, or DSCP Priority of a frame matching the defined ACL rule. (This feature is commonly referred to as ACL packet marking.) Use the **no** form to remove the ACL marker.

Syntax

match access-list ip *acl_name* [**set priority** *priority*] {**set tos** *tos_value* | **set dscp** *dscp_value*}

no match access-list ip *acl_name*

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- *priority* – Class of Service value in the IEEE 802.1p priority tag. (Range: 0-7; 7 is the highest priority)
- tos_value – IP Precedence value. (Range: 0-7)
- *dscp_value* – Differentiated Services Code Point value. (Range: 0-63)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- You must configure an ACL mask before you can change frame priorities based on an ACL rule.
- Traffic priorities may be included in the IEEE 802.1p priority tag. This tag is also incorporated as part of the overall IEEE 802.1Q VLAN tag. To specify this priority, use the **set priority** keywords.

 © 2004 Foundry Networks, Inc.

- The IP frame header also includes priority bits in the Type of Service (ToS) octet. The Type of Service octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. To specify the IP precedence priority, use the **set tos** keywords. To specify the DSCP priority, use the **set dscp** keywords. Note that the IP frame header can include either the IP Precedence or DSCP priority type.
- The precedence for priority mapping by this switch is IP Precedence or DSCP Priority, and then 802.1p priority.

Example

```
Console(config)#interface ethernet 1/12
Console(config-if)#match access-list ip bill set dscp 0
Console(config-if)#
```

Related Commands

show marking (4-80)

show marking

This command displays the current configuration for packet marking.

Command Mode

Privileged Exec

Example

```
Console#show marking
Interface ethernet 1/12
 match access-list IP bill set DSCP 0
 match access-list MAC a set priority 0
Console#
```

Related Commands

match access-list ip (4-79)

MAC ACLs

Command	Function	Mode	Page
access-list mac	Creates a MAC ACL and enters configuration mode	GC	4-81
permit, deny	Filters packets matching a specified source and destination address, packet format, and Ethernet type	MAC-ACL	4-81
show mac access-list	Displays the rules for configured MAC ACLs	PE	4-83
access-list mac mask-precedence	Changes to the mode for configuring access control masks	GC	4-83
mask	Sets a precedence mask for the ACL rules	MAC-Mask	4-84
show access-list mac mask-precedence	Shows the ingress or egress rule masks for MAC ACLs	PE	4-85
permit/deny offset	Filters packets matching a pattern starting at the offset	MAC-ACL	4-86
mac access-group	Adds a port to a MAC ACL	IC	4-87
show mac access-group	Shows port assignments for MAC ACLs	PE	4-87

© 2004 Foundry Networks, Inc.

Command	Function	Mode	Page
map access-list mac	Sets the CoS value and corresponding output queue for packets matching an ACL rule	IC	4-88
show map access-list mac	Shows CoS value mapped to an access list for an interface	PE	4-89
match access-list mac	Changes the 802.1p priority the priority of a frame matching the defined rule (i.e., also called packet marking)	IC	4-89
show marking	Displays the current configuration for packet marking	PE	4-90

access-list mac

This command adds a MAC access list and enters MAC ACL configuration mode. Use the **no** form to remove the specified ACL.

Syntax

[**no**] **access-list mac** *acl_name*

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- An egress ACL must contain all deny rules.
- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

Related Commands

permit, deny 4-81
mac access-group (4-87)
show mac access-list (4-83)

permit, deny (MAC ACL)

This command adds a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Use the **no** form to remove a rule.

© 2004 Foundry Networks, Inc.

Syntax

[**no**] {**permit** | **deny**}
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

Note: - The default is for Ethernet II packets.

[**no**] {**permit** | **deny**} **tagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**no** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

[**no**] {**permit** | **deny**} **untagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**ethertype** *protocol* [*protocol-bitmask*]]

[**no**] {**permit** | **deny**} **tagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*]

[**no**] {**permit** | **deny**} **untagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}

- **tagged-eth2** – Tagged Ethernet II packets.
- **untagged-eth2** – Untagged Ethernet II packets.
- **tagged-802.3** – Tagged Ethernet 802.3 packets.
- **untagged-802.3** – Untagged Ethernet 802.3 packets.
- **any** – Any MAC source or destination address.
- **host** – A specific MAC address.
- *source* – Source MAC address.
- *destination* – Destination MAC address range with bitmask.
- *address-bitmask** – Bitmask for MAC address (in hexidecimal format).
- vid – VLAN ID. (Range: 1-4095)
- *vid-bitmask** – VLAN bitmask. (Range: 1-4095)
- *protocol* – A specific Ethernet protocol number. (Range: 600-fff hex.)
- *protocol-bitmask** – Protocol bitmask. (Range: 600-fff hex.)

* For all bitmasks, “1” means care and “0” means ignore.

Default Setting

None

Command Mode

MAC ACL

 © 2004 Foundry Networks, Inc.

Command Usage

- New rules are added to the end of the list.
- The **ethertype** option can only be used to filter Ethernet II formatted packets.
- A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:
  - 0800 - IP
  - 0806 - ARP
  - 8137 - IPX

Example

This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de
   ethertype 0800
Console(config-mac-acl)#
```

Related Commands

access-list mac (4-81)

show mac access-list

This command displays the rules for configured MAC ACLs.

Syntax

show mac access-list [*acl_name*]

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show mac access-list
MAC access-list jerry:
  permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

Related Commands

permit, deny 4-81
mac access-group (4-87)

access-list mac mask-precedence

This command changes to MAC Mask mode used to configure access control masks. Use the **no** form to delete the mask table.

Syntax

[**no**] **access-list ip mask-precedence** {**in** | **out**}

- **in** – Ingress mask for ingress ACLs.
- **out** – Egress mask for egress ACLs.

Default Setting

Default system mask: Filter inbound packets according to specified MAC ACLs.

 © 2004 Foundry Networks, Inc.

Command Mode

Global Configuration

Command Usage

- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
- A mask can only be used by all ingress ACLs or all egress ACLs.
- The precedence of the ACL rules applied to a packet is not determined by order of the rules, but instead by the order of the masks; i.e., the first mask that matches a rule will determine the rule that is applied to a packet.

Example

```
Console(config)#access-list mac mask-precedence in
Console(config-mac-mask-acl)#
```

Related Commands

mask (MAC ACL) (4-84)
mac access-group (4-87)

mask (MAC ACL)

This command defines a mask for MAC ACLs. This mask defines the fields to check in the packet header. Use the **no** form to remove a mask.

Syntax

[**no**] **mask** [**pktformat**]
{**any** | **host** | *source-bitmask*} {**any** | **host** | *destination-bitmask*}
[**vid** [*vid-bitmask*]] [**ethertype** [*ethertype-bitmask*]]

- **pktformat** – Check the packet format field. (If this keyword must be used in the mask, the packet format must be specified in ACL rule to match.)
- **any** – Any address will be matched.
- **host** – The address must be for a single node.
- *source-bitmask* – Source address of rule must match this bitmask.
- destination-bitmask – Destination address of rule must match this bitmask.
- **vid** – Check the VLAN ID field.
- *vid-bitmask* – VLAN ID of rule must match this bitmask.
- **ethertype** – Check the Ethernet type field.
- *ethertype-bitmask* – Ethernet type of rule must match this bitmask.

Default Setting

None

Command Mode

MAC Mask

Command Usage

- Up to seven masks can be assigned to an ingress or egress ACL.
- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules were entered.

 © 2004 Foundry Networks, Inc.

- First create the required ACLs and inbound or outbound masks before mapping an ACL to an interface.

Example

This example shows how to create an Ingress MAC ACL and bind it to a port. You can then see that the order of the rules have been changed by the mask.

```
Console(config)#access-list mac M4
Console(config-mac-acl)#permit any any
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11 ff-ff-ff-ff-ff-ff
any vid 3
Console(config-mac-acl)#end
Console#show access-list
MAC access-list M4:
  permit any any
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
Console(config)#access-list mac mask-precedence in
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#mac access-group M4 in
Console(config-if)#end
Console#show access-list
MAC access-list M4:
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
  permit any any
MAC ingress mask ACL:
  mask pktformat host any vid
Console#
```

This example creates an Egress MAC ACL.

```
Console(config)#access-list mac M5
Console(config-mac-acl)#deny tagged-802.3 host 00-11-11-11-11-11 any
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11 ff-ff-ff-ff-ff-ff
any vid 3 ethertype 0806
Console(config-mac-acl)#end
Console#show access-list
MAC access-list M5:
  deny tagged-802.3 host 00-11-11-11-11-11 any
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3 ethertype 0806
Console(config)#access-list mac mask-precedence out
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/5
Console(config-if)#mac access-group M5 out
Console(config-if)#end
Console#show access-list
MAC access-list M5:
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3 ethertype 0806
  deny tagged-802.3 host 00-11-11-11-11-11 any
MAC ingress mask ACL:
  mask pktformat host any vid ethertype
Console#
```

show access-list mac mask-precedence

This command shows the ingress or egress rule masks for MAC ACLs.

Syntax

show access-list mac mask-precedence [**in** | **out**]

- **in** – Ingress mask precedence for ingress ACLs.
- **out** – Egress mask precedence for egress ACLs.

Command Mode

Privileged Exec

© 2004 Foundry Networks, Inc.

Example

```
Console#show access-list mac mask-precedence
MAC egress mask ACL:
  mask pktformat host any vid ethertype
Console#
```

Related Commands

mask (MAC ACL) (4-84)

permit offset, deny offset (MAC ACL)

Use this command to add a rule to a MAC ACL. The rule fliters packets matching the specified data pattern starting at the offset. Use the **no** form to remove a rule.

Syntax

{**permi**t | **deny**} **offset** *offset_value length bitmask data*

no {**permit** | **deny**} **offset** *offset_value length bitmask data*

- *offset_value* – Byte offset from the beginning of the frame.
- *length* – Length of the data pattern to match.
- bitmask – Decimal number representing the data bits to match.
- *data* – Data to match, entered as a sequence of hexadecimal letters with no separators.

Default Setting

None

Command Mode

MAC ACL

Command Usage

- This command is used to filter frames that match a specified pattern, and can be used to filter traffic associated with precisely defined events.
- The bitmask is a decimal number (representing an equivalent bit mask) that is applied to the data. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit.
- Packet filtering based on arbitrary offsets and data patterns can adversely affect switch throughput. Try to avoid using packet filtering based on pattern matching unless this is absolutely necessary to solve a specific problem.

Example

This example shows how to filter any Ethernet II packets directed to the IP address 10.1.0.23 that havethe Don’t Fragment flag set.

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#permit offset ???
```

Related Commands

mac access-group (4-87)
show mac access-list (4-83)

 © 2004 Foundry Networks, Inc.

mac access-group

This command binds a port to a MAC ACL. Use the **no** form to remove the port.

Syntax

mac access-group *acl_name* {**in** | **out**}

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- **in** – Indicates that this list applies to ingress packets.
- **out** – Indicates that this list applies to egress packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.

Example

```
Console(config)#interface ethernet 1/25
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

Related Commands

show mac access-list (4-83)

show mac access-group

This command shows the ports assigned to MAC ACLs.

Command Mode

Privileged Exec

Example

```
Console#show mac access-group
Interface ethernet 1/5
 MAC access-list M5 out
Console#
```

Related Commands

mac access-group (4-87)

© 2004 Foundry Networks, Inc.

map access-list mac

This command sets the output queue for packets matching an ACL rule. The specified CoS value is only used to map the matching packet to an output queue; it is not written to the packet itself. Use the **no** form to remove the CoS mapping.

Syntax

[**no**] **map access-list mac** *acl_name* **cos** *cos-value*

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- *cos-value* – CoS value. (Range: 0-7)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- You must configure an ACL mask before you can map CoS values to the rule.
- A packet matching a rule within the specified ACL is mapped to one of the output queues as shown below.

EdgeIron 24G-A, 48G								
Priority	1	2	4	6	8	10	12	14
Queue	0	1	2	3	4	5	6	7

EdgeIron 4802CF, 2402CF				
Priority	1	4	16	64
Queue	0	1	2	3

EdgeIron 24G				
Priority	16	64	128	240
Queue	0	1	2	3

Example

```
Console(config)#int eth 1/5
Console(config-if)#map access-list mac M5 cos 0
Console(config-if)#
```

Related Commands

queue cos-map (4-167)
show map access-list mac (4-89)

© 2004 Foundry Networks, Inc.

show map access-list mac

This command shows the CoS value mapped to a MAC ACL for the current interface. (The CoS value determines the output queue for packets matching an ACL rule.)

Syntax

show map access-list mac [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.

Command Mode

Privileged Exec

Example

```
Console#show map access-list mac
Access-list to COS of Eth 1/5
 Access-list M5 cos 0
Console#
```

Related Commands

map access-list mac (4-88)

match access-list mac

This command changes the IEEE 802.1p priority of a Layer 2 frame matching the defined ACL rule. (This feature is commonly referred to as ACL packet marking.) Use the **no** form to remove the ACL marker.

Syntax

match access-list mac *acl_name* **set priority** *priority*

no match access-list mac *acl_name*

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- *priority* – Class of Service value in the IEEE 802.1p priority tag. (Range: 0-7; 7 is the highest priority)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

You must configure an ACL mask before you can change frame priorities based on an ACL rule.

Example

```
Console(config)#interface ethernet 1/12
Console(config-if)#match access-list mac a set priority 0
Console(config-if)#
```

Related Commands

show marking (4-80)

© 2004 Foundry Networks, Inc.

ACL Information

Command	Function	Mode	Page
show access-list	Show all ACLs and associated rules	PE	4-90
show access-group	Shows the ACLs assigned to each port	PE	4-90

show access-list

This command shows all ACLs and associated rules, as well as all the user-defined masks.

Command Mode

Privileged Exec

Command Usage

Once the ACL is bound to an interface (i.e., the ACL is active), the order in which the rules are displayed is determined by the associated mask.

Example

```
Console#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 0.0.15.255
IP extended access-list bob:
  permit 10.7.1.1 0.0.0.255 any
  permit 192.168.1.0 0.0.0.255 any dport 80
  permit 192.168.1.0 0.0.0.255 any protocol tcp control-code 2 2
MAC access-list jerry:
  permit any 00-30-29-94-34-de ethertype 800
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#
```

show access-group

This command shows the port assignments of ACLs.

Command Mode

Privileged Executive

Example

```
Console#show access-group
Interface ethernet 1/25
 IP standard access-list david
 MAC access-list jerry
Console#
```


© 2004 Foundry Networks, Inc.

SNMP Commands

Controls access to this switch from SNMP management stations, as well as the error types sent to trap managers.

Command	Function	Mode	Page
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC	4-91
snmp-server contact	Sets the system contact string	GC	4-92
snmp-server location	Sets the system location string	GC	4-92
snmp-server host	Specifies the recipient of an SNMP notification operation	GC	4-93
snmp-server enable traps	Enables the device to send SNMP notifications (i.e., SNMP traps)	GC	4-94
snmp ip filter	Sets IP addresses of clients allowed to management access to the switch via SNMP	GC	4-94
show snmp	Displays the status of SNMP communications	NE, PE	4-95

snmp-server community

Use this command to define the community access string for the Simple Network Management Protocol. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro**|**rw**]
no snmp-server community *string*

- *string* - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- public - Read-only access. Authorized management stations are only able to retrieve MIB objects.
- private - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Command Usage

The first snmp-server community command you enter enables SNMP (SNMP v1 and v2c). The **no** snmp-server community command disables all versions of SNMP.

Example

```
Console(config)#snmp-server community alpha rw
Console(config)#
```


© 2004 Foundry Networks, Inc.

snmp-server contact

Use this command to set the system contact string. Use the **no** form to remove the system contact information.

Syntax

snmp-server contact *string*
no snmp-server contact

string - String that describes the system contact information. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server contact Paul
Console(config)#
```

Related Commands

snmp-server location

snmp-server location

Use this command to set the system location string. Use the **no** form to remove the location string.

Syntax

snmp-server location *text*
no snmp-server location

text - String that describes the system location.
(Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server location WC-19
Console(config)#
```

Related Commands

snmp-server contact (4-92)

© 2004 Foundry Networks, Inc.

snmp-server host

Use this command to specify the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

Syntax

snmp-server host *{host-addr community-string}* [**version 1** | **2c**]
no snmp-server host *host-addr*

- *host-addr* - Name or Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)
- *community-string* - Password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command prior to using the **snmp-server host** command.
  (Maximum length: 32 characters)
- **version** - Specifies whether to send notifications as SNMP v1 or SNMP v2c traps.

Default Setting

Host Address: None
SNMP Version: 1

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host.
- The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.
- The switch can send SNMP version 1 or version 2c traps to a host IP address, depending on the SNMP version that the management station supports. If the **snmp-server host** command does not specify the SNMP version, the default is to send SNMP version 1 traps.
- Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled.

Example

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

Related Commands

snmp-server enable traps

© 2004 Foundry Networks, Inc.

snmp-server enable traps

Use this command to enable this device to send Simple Network Management Protocol traps (SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

snmp-server enable traps [**authentication** | **link-up-down**]
no snmp-server enable traps [**authentication** | **link-up-down**]

- **authentication** - Keyword to issue authentication failure traps.
- **link-up-down** - Keyword to issue link-up or link-down traps.

Default Setting

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.
- The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

Example

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Related Commands

snmp-server host (4-93)

snmp ip filter

Sets the IP addresses of clients that are allowed management access to the switch via SNMP. Use the **no** form of this command to remove an IP address.

Syntax

snmp ip filter *ip_address subnet_mask*
no snmp ip filter *ip_address subnet_mask*

- *ip_address* - An IP address indicating a client or group of clients that are allowed SNMP access to the switch.
- *subnet_mask* - An address bitmask of decimal numbers that represent the address bits to match.

Default Setting

None

 © 2004 Foundry Networks, Inc.

Command Mode

Global Configuration

Command Usage

- You can create a list of up to 16 IP addresses or IP address groups that are allowed access to the switch via SNMP management software.
- Address bitmasks are similar to a subnet mask, containing four decimal integers from 0 to 255, each separated by a period. The binary mask uses “1” bits to indicate “match” and “0” bits to indicate “ignore.”
- If the IP is the address of a single management station, the bitmask should be set to 255.255.255.255. Otherwise, the IP address group is specified by the bitmask.
- The default setting is null, which allows all IP groups SNMP access to the switch. If one IP address is configured, the IP filtering is enabled and only addresses in the IP group will have SNMP access.
- IP filtering does not affect management access to the switch using the Web interface or Telnet.

Example

The following example enables SNMP IP filtering on the switch and allows SNMP management access to client IP 10.1.2.3, and client IP group 10.1.3.0 to 10.1.3.255.

```
Console(config)#snmp ip filter 10.1.2.3 255.255.255.255
Console(config)#snmp ip filter 10.1.3.0 255.255.255.0
Console(config)#
```

Related Commands

show snmp (4-95)

show snmp

Use this command to check the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the **snmp-server enable traps** command.

© 2004 Foundry Networks, Inc.

Example

```
Console#show snmp

SNMP traps:
 Authentication: enable
   Link-up-down: enable

SNMP communities:
   1. private, and the privilege is read-write
   2. public, and the privilege is read-only

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
   0 Trap PDUs

SNMP logging: disabled
SNMP ip filter group:
    1. IP:10.1.2.3 Mask:255.255.255.255 valid
    2. IP:10.1.3.0 Mask:255.255.255.0 valid
Console#
```

IP Commands

An IP address may be used for management access to the switch over your network. By default, the switch uses DHCP to assign IP settings to VLAN 1 on the switch. If you wish to manually configure IP settings, you need to change the switch's user-specified defaults (IP address 0.0.0.0 and netmask 255.0.0.0) to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment.

Command	Function	Mode	Page
ip address	Sets the IP address for this device	IC	4-97
ip dhcp restart	Submits a BOOTP or DCHP client request	PE	4-98
ip default-gateway	Defines the default gateway through which an in-band management station can reach this device	GC	4-98
show ip interface	Displays the IP settings for this device	PE	4-99
show ip redirects	Displays the default gateway configured for this device	PE	4-99
ping	Sends ICMP echo request packets to another node on the network	NE, PE	4-100

 © 2004 Foundry Networks, Inc.

ip address

Use this command to set the IP address for this device. Use the **no** form to restore the default IP address.

Syntax

ip address {*ip-address netmask* | **bootp** | **dhcp**}
no ip address

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **bootp** - Obtains IP address from BOOTP.
- **dhcp** - Obtains IP address from DHCP.

Default Setting

IP address: 0.0.0.0
Netmask: 255.0.0.0

Command Mode

Interface Configuration (VLAN)

Command Usage

- You must assign an IP address to this device to gain management access over the network. You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.
- If you select the **bootp** or **dhcp** option, IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).
- You can start broadcasting BOOTP or DHCP requests by entering an **ip dhcp restart** command, or by rebooting the switch.

Note: Only one VLAN interface can be assigned an IP address (the default is VLAN 1). This defines the management VLAN, the only VLAN through which you can gain management access to the switch. If you assign an IP address to any other VLAN, the new IP address overrides the original IP address and this becomes the new management VLAN.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

Related Commands

ip dhcp restart

© 2004 Foundry Networks, Inc.

ip dhcp restart

Use this command to submit a BOOTP or DCHP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- DHCP requires the server to reassign the client's last address if available.
- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart
Console#show ip interface
IP interface vlan
 IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
 and address mode: Dhcp.
Console#
```

Related Commands

ip address (4-97)

ip default-gateway

Use this command to a establish a static route between this device and management stations that exist on another network segment. Use the **no** form to remove the static route.

Syntax

ip default-gateway *gateway*
no ip default-gateway

gateway - IP address of the default gateway

Default Setting

No static route is established.

Command Mode

Global Configuration

Command Usage

A gateway must be defined if the management station is located in a different IP segment.

Example

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
```

 © 2004 Foundry Networks, Inc.

Related Commands

show ip redirects (4-99)

show ip interface

Use this command to display the settings of an IP interface.

Default Setting

All interfaces

Command Mode

Privileged Exec

Command Usage

This switch can only be assigned one IP address. This address is used for managing the switch.

Example

```
Console#show ip interface
 IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#
```

Related Commands

show ip redirects

show ip redirects

Use this command to show the default gateway configured for this device.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

Related Commands

ip default-gateway (4-98)

© 2004 Foundry Networks, Inc.

ping

Use this command to send ICMP echo request packets to another node on the network.

Syntax

ping *host* [**count** *count*][**size** *size*]

- *host* - IP address or IP alias of the host.
- *count* - Number of packets to send. (Range: 1-16, default: 5)
- *size* - Number of bytes in a packet. (Range: 32-512, default: 32)
  The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

Default Setting

This command has no default for the host.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- Following are some results of the ping command:
  - *Normal response* -The normal response occurs in one to ten seconds, depending on network traffic.
  - *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.
  - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
  - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- Press <Esc> to stop pinging.

Example

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

Related Commands

interface (4-109)

 © 2004 Foundry Networks, Inc.

Line Commands

You can access the onboard configuration program by attaching a VT100 compatible device to the server's serial port. These commands are used to set communication parameters for the serial port or a virtual terminal. Note that Telnet is considered a virtual terminal connection, and the only commands that apply to Telnet include **exec-timeout** and **password-thresh**.

Command	Function	Mode	Page
line	Identifies a specific line for configuration and starts the line configuration mode	GC	4-101
login	Enables password checking at login	LC	4-102
password	Specifies a password on a line	LC	4-103
exec-timeout	Sets the interval that the command interpreter waits until user input is detected	LC	4-103
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC	4-104
silent-time	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command	LC	4-105
databits	Sets the number of data bits per character that are interpreted and generated by hardware	LC	4-105
parity	Defines the generation of a parity bit	LC	4-106
speed	Sets the terminal baud rate	LC	4-106
stopbits	Sets the number of the stop bits transmitted per byte	LC	4-107
show line	Displays a terminal line's parameters	NE, PE	4-107

line

Use this command to identify a specific line for configuration, and to process subsequent line configuration commands.

Syntax

line {**console** | **vty**}

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access.

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

Telnet is considered a virtual terminal connection and will be shown as "Vty" in screen displays such as **show users**. However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

© 2004 Foundry Networks, Inc.

Example

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

Related Commands

show line (4-107)
show users (4-47)

login

Use this command to enable password checking at login. Use the **no** form to disable password checking and allow connections without a password.

Syntax

login [**local**]
no login

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Default Setting

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Command Mode

Line Configuration

Command Usage

- There are three authentication modes provided by the switch itself at login:
  - **login** selects authentication by a single global password as specified by the **password** line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
  - **login local** selects authentication via the user name and password specified by the **username** command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).
  - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.
- This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS software installed on those servers.

Example

```
Console(config-line)#login local
Console(config-line)#
```

Related Commands

username (4-20)
password

 © 2004 Foundry Networks, Inc.

password

Use this command to specify the password for a line. Use the **no** form to remove the password.

Syntax

password {**0** | **7**} *password*
no password

- {**0** | **7**} - 0 means plain password, 7 means encrypted password
- *password* - Character string that specifies the line password. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

- When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the **password-thresh** command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.
- The encrypted password is required for compatiblity with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Related Commands

login (4-102)
password-thresh (4-104)

exec-timeout

Use this command to set the interval that the system waits until user input is detected. Use the **no** form to remove the timeout definition.

Syntax

exec-timeout *seconds*
no exec-timeout

seconds - Integer that specifies the number of seconds. (Range: 0 - 65535 seconds; 0: no timeout)

Default Setting

CLI: No timeout
Telnet: 10 minutes

Command Mode

Line Configuration

 © 2004 Foundry Networks, Inc.

Command Usage

- If input is detected, the system resumes the current connection; or if no connections exist, it returns the terminal to the idle state and disconnects the incoming session.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

password-thresh

Use this command to set the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

Syntax

password-thresh *threshold*
no password-thresh

threshold - The number of allowed password attempts. (Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

- When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the **silent-time** command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.
- This command applies to both the local console and Telnet connections.

Example

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

Related Commands

silent-time

 © 2004 Foundry Networks, Inc.

silent-time

Use this command to set the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command. Use the **no** form to remove the silent time value.

Syntax

silent-time *seconds*
no silent-time

seconds - The number of seconds to disable console response. (Range: 0-65535; 0: no silent-time)

Default Setting

The default value is no silent-time.

Command Mode

Line Configuration

Command Usage

If the password threshold was not set with the **password-thresh** command, silent-time begins after the default value of three failed logon attempts.

Example

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

Related Commands

password-thresh (4-104)

databits

Use this command to set the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

Syntax

databits {**7** | **8**}
no databits

- 7 - Seven data bits per character.
- 8 - Eight data bits per character.

Default Setting

8 data bits per character

Command Mode

Line Configuration

Command Usage

The **databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

© 2004 Foundry Networks, Inc.

Example

To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

Related Commands

parity

parity

Use this command to define generation of a parity bit. Use the **no** form to restore the default setting.

Syntax

parity {**none** | **even** | **odd**}
no parity

- **none** - No parity
- **even** - Even parity
- **odd** - Odd parity

Default Setting

No parity

Command Mode

Line Configuration

Command Usage

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Example

To specify no parity, enter this command:

```
Console(config-line)#parity none
Console(config-line)#
```

speed

Use this command to set the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

Syntax

speed *bps*
no speed

bps - Baud rate in bits per second.
(Options: 9600, 57600, 38400, 19200, 115200 bps)

Default Setting

9600 bps

 © 2004 Foundry Networks, Inc.

Command Mode

Line Configuration

Command Usage

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported.

Example

To specify 57600 bps, enter this command:

```
Console(config-line)#speed 57600
Console(config-line)#
```

stopbits

Use this command to set the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

Syntax

stopbits {**1** | **2**}

- 1 - One stop bit
- 2 - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

show line

Use this command to display the terminal line's parameters.

Syntax

show line [**console** | **vty**]

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access.

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

 © 2004 Foundry Networks, Inc.

Example

To show all lines, enter this command:

```
Console#show line
 Console configuration:
  Password threshold: 3 times
  Interactive timeout: Disabled
  Silent time: Disabled
  Baudrate: 9600
  Databits: 8
  Parity: none
  Stopbits: 1

Vty configuration:
  Password threshold: 3 times
  Interactive timeout: 65535
Console#
```

Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

Command	Function	Mode	Page
interface	Configures an interface type and enters interface configuration mode	GC	4-109
description	Adds a description to an interface configuration	IC	4-109
speed-duplex	Configures the speed and duplex operation of a given interface when auto-negotiation is disabled	IC	4-110
negotiation	Enables auto-negotiation of a given interface	IC	4-110
capabilities	Advertises the capabilities of a given interface for use in auto-negotiation	IC	4-111
flowcontrol	Enables flow control on a given interface	IC	4-112
shutdown	Disables an interface	IC	4-113
switchport broadcast	Configures broadcast storm control	IC	4-114
port security	Enables port security on an interface.	IC	4-114
port security (EdgeIron 2402CF)	Enables port security on an interface.	IC	4-116
clear counters	Clears statistics on an interface	PE	4-117
show interfaces status	Displays status for the specified interface	NE, PE	4-117
show interfaces counters	Displays statistics for the specified interface	NE, PE	4-118
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	4-119

 © 2004 Foundry Networks, Inc.

interface

Use this command to configure an interface type and enter interface configuration mode. Use the **no** form to remove a trunk.

Syntax

interface *interface*
no interface port-channel *channel-id*

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)
- **vlan** *vlan-id* (Range: 1-4094)

Default Setting

None

Command Mode

Global Configuration

Example

To specify the Ethernet port, enter the following command:

```
Console(config)#interface ethernet 1/25
Console(config-if)#
```

description

Use this command to add a description to an interface. Use the **no** form to remove the description.

Syntax

description *string*
no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following example adds a description to Ethernet port 15.

```
Console(config)#interface ethernet 1/15
Console(config-if)#description RD-SW#3
Console(config-if)#
```


© 2004 Foundry Networks, Inc.

speed-duplex

Use this command to configure the speed and duplex mode of a given interface when auto-negotiation is disabled. Use the **no** form to restore the default.

Syntax

speed-duplex {**1000full** | **100full** | **100half** | **10full** | **10half**}
no speed-duplex

- **1000full** - Forces 1000 Mbps full-duplex operation
- **100full** - Forces 100 Mbps full-duplex operation
- **100half** - Forces 100 Mbps half-duplex operation
- **10full** - Forces 10 Mbps full-duplex operation
- **10half** - Forces 10 Mbps half-duplex operation

Default Setting

- Auto-negotiation is enabled by default.
- When auto-negotiation is disabled, the default speed-duplex setting is 1000full for Gigabit Ethernet ports.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- To force operation to the speed and duplex mode specified in a speed-duplex command, use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To set the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

Example

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (4-110)
capabilities (4-111)

negotiation

Use this command to enable auto-negotiation for a given interface. Use the **no** form to disable auto-negotiation.

Syntax

negotiation
no negotiation

Default Setting

Enabled

 © 2004 Foundry Networks, Inc.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.
- If auto-negotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

Note: Auto MDI/MDIX cannot work at forced mode.

Example

The following example configures port 11 to use auto-negotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
```

Related Commands

capabilities (4-111)
speed-duplex (4-110)
flowcontrol (4-112)

capabilities

Use this command to advertise the port capabilities of a given interface during auto-negotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

Syntax

capabilities {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}

no port-capabilities [**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**]

- **1000full** - Supports 1000 Mbps full-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation
- **10full** - Supports 10 Mbps full-duplex operation
- **10half** - Supports 10 Mbps half-duplex operation
- **flowcontrol** - Supports flow control
- **symmetric** (Gigabit only) - When specified, the port transmits and receives pause frames; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames. (The current switch ASIC only supports symmetric pause frames.)

Note: Flow control setting applies only to forced-mode configuration. The auto-negotiation behavior is dependent on a port's capability setting.

© 2004 Foundry Networks, Inc.

Default Setting

- 100BASE-TX: 10half, 10full, 100half, 100full
- 1000BASE-T: 10half, 10full, 100half, 100full, 1000full
- 1000BASE-SX/LX/LH: 1000full

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When auto-negotiation is enabled with the **negotiation** command, the switch will negotiate the best settings for a link based on the **capabilites** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.

Example

The following example configures Ethernet port 5 capabilities to 100half, 100full and flow control.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

Related Commands

speed-duplex (4-110)
negotiation (4-110)
flowcontrol (4-112)

flowcontrol

Use this command to enable flow control. Use the **no** form to disable flow control.

Syntax

flowcontrol
no flowcontrol

Default Setting

Flow control enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port.
- To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.

 © 2004 Foundry Networks, Inc.

- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.
- Due to a hardware limitation, flow control only works on those ports located in the same chip (ports 1-24, 49 and ports 25-48, 50). Cross-chip flow control does not work.

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

capabilities (4-111)
negotiation (4-110)

shutdown

Use this command to disable an interface. To restart a disabled interface, use the **no** form.

Syntax

shutdown
no shutdown

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```


© 2004 Foundry Networks, Inc.

switchport broadcast

Use this command to configure broadcast storm control. Use the **no** form to disable broadcast storm control.

Syntax

switchport broadcast packet-rate *rate*
no switchport broadcast

rate - Threshold level as a rate; i.e., packets per second.
(Range – EdgeIron 4802CF, 2402CF: 500 - 262143;
EdgeIron 24G-A, 24G, 48G: 16, 64, 128, 256)

Default Setting

Enabled for all ports
Packet-rate limit – EdgeIron 4802CF, 2402CF: 500 packets per second;
EdgeIron 24G-A, 24G, 48G: 256 packets per second

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When broadcast traffic exceeds the specified threshold, packets above that threshold are dropped.
- This command can enable or disable broadcast storm control for the selected interface. However, the specified threshold value applies to all ports on the switch.
- Enabling jumbo frames for the EdgeIron 24G-A will limit the maximum threshold for broadcast storm control to 64 packets per second.

Example

The following shows how to configure broadcast storm control at 600 packets per second on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

port security

Use this command to enable and configure port security on a port. Use the **no** form to disable port security or reset the intrusion action to the default.

Syntax

port security [**action** {**shutdown** | **trap** | **trap-and-shutdown**}]
no port security [**action**]

- **action** - Indicates the security action to be taken when a port security violation is detected.
  - shutdown - Disable the port only.
  - trap - Issue an SNMP trap message only.
  - trap-and-shutdown - Issue an SNMP trap message and disable the port.

Default Setting

Status: Disabled
Action: None

 © 2004 Foundry Networks, Inc.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- If you enable port security, the switch will stop dynamically learning new addresses on the specified port. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.
- To use port security, first allow the switch to dynamically learn the <source MAC address, VLAN> pair for frames received on a port for an initial training period, and then enable port security to stop address learning. Be sure you enable the learning function long enough to ensure that all valid VLAN members have been registered on the selected port.
- To add new VLAN members at a later time, you can manually add secure addresses with the **mac-address-table static** command, or turn off port security to reenable the learning function long enough for new VLAN members to be registered. Learning may then be disabled again, if desired, for security.
- A secure port has the following restrictions:
  - Cannot be connected to a network interconnection device.
  - Cannot be a member of a static trunk.
  - It can be configured as an LACP trunk port, but the switch does not allow the LACP trunk to be enabled.
- A port that is already configured as an LACP or static trunk port cannot be enabled as a secure port.
- If a port is disabled due to a security violation, it must be manually re-enabled by using the **no shutdown** command.
- EdgeIron 24G-A, 24G, 48G restrictions:
  - The switch only supports the **trap-and-shutdown** security action.
  - Although the **port security action** command is an Interface Configuration command, it applies globally to all switch ports.

Example

This example sets the port security action for the switch and enables port security for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown
Console(config-if)#port security
Console(config-if)#
```

Related Commands

shutdown (4-113)
mac-address-table static (4-121)

© 2004 Foundry Networks, Inc.

port security (EdgeIron 2402CF)

Use this command to enable and configure port security on a port. Use the **no** form to disable port security and reset the maximum addresses to the default.

Syntax

port security [**max-mac-count** *address-number*]
no port security [**max-mac-count**]

address-number - Sets the maximum number of MAC addresses that can be learned on a port. (Range: 0 - 20)

Default Setting

Status: Disabled

Maximum Addresses: 0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- If you enable port security on a specified port, the switch will dynamically learn MAC addresses until the specified number has been reached and then stop. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.
- To use port security, specify a maximum number of addresses to allow on the port and then let the switch dynamically learn the <source MAC address, VLAN> pair for frames received on the port. You can also manually add secure addresses to the port with the **mac-address-table static** command.
- First use the **port security max-mac-count** command to set the number of addresses, and then use the **port security** command to enable security on the port.
- Use the **no port security max-mac-count** command to disable port security and reset the maximum number of addresses to the default.
- A secure port has the following restrictions:
  - Cannot be connected to a network interconnection device.
  - Cannot be a member of a static trunk.
  - It can be configured as an LACP trunk port, but the switch does not allow the LACP trunk to be enabled.
- A port that is already configured as an LACP or static trunk port cannot be enabled as a secure port.
- Note that the EdgeIron 2402CF does not provide an intrusion action to shutdown a port or send an SNMP trap message.

Example

This example sets the maximum MAC addresses and enables port security for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security max-mac-count 10
Console(config-if)#port security
Console(config-if)#
```

Related Commands

mac-address-table static (4-121)

 © 2004 Foundry Networks, Inc.

clear counters

Use this command to clear statistics on an interface.

Syntax

clear counters *interface*

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on port 5.

```
Console#clear counters ethernet 1/5
Console#
```

show interfaces status

Use this command to display the status for an interface.

Syntax

show interfaces status *interface*

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)
- **vlan** *vlan-id* (Range: 1-4094)

Default Setting

Shows the status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

 © 2004 Foundry Networks, Inc.

Command Usage

- If no interface is specified, information on all interfaces is displayed.
- For a description of the items displayed by this command, see “Displaying Connection Status” on page 3-52.

Example

```
Console#show interface status ethernet 1/5
Information of Eth 1/5
 Basic information:
  Port type: 100TX
  Mac address: 00-30-F1-47-58-3F
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Broadcast storm: Enabled
  Broadcast storm limit: 500 packets/second
  Flow control: Disabled
  Lacp: Disabled
  Port security: Disabled
  Port security action: None
 Current status:
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 100full
  Flow control type: None
Console#
```

show interfaces counters

Use this command to display statistics for an interface.

Syntax

show interfaces counters [*interface* | **brief**]

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)
- **brief** - Displays brief information for all ports.

Default Setting

Shows the counters for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- If no interface is specified, information on all interfaces is displayed.
- For a description of the items displayed by this command, see “Showing Device Statistics” on page 3-120.

 © 2004 Foundry Networks, Inc.

Example

```
Console#show interfaces counters ethernet 1/7
Ethernet 1/ 7
 Iftable stats:
  Octets input: 30658, Octets output: 196550
  Unicast input: 6, Unicast output: 5
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 3064
  Broadcast input: 262, Broadcast output: 1
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 227208, Packets: 3338
  Broadcast pkts: 263, Multi-cast pkts: 3064
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 3150, Packet size 65 to 127 octets: 139
  Packet size 128 to 255 octets: 49, Packet size 256 to 511 octets: 0
  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

This example displays brief information for all ports.

```
Console#show interfaces counters brief
Ethernet       Packets          Collision        Errors
Port      [Receive Transmit]   [Receive]    [Input Output]
1/ 1         0        0          0           0     0
1/ 2         0        0          0           0     0
1/ 3         0        0          0           0     0
1/ 4         0        0          0           0     0
1/ 5         0        0          0           0     0
1/ 6         0        0          0           0     0
1/ 7         0        0          0           0     0
1/ 8         0        0          0           0     0
1/ 9         0        0          0           0     0
1/10         0        0          0           0     0
1/11         0        0          0           0     0
1/12         0        0          0           0     0
1/13         0        0          0           0     0
1/14         0        0          0           0     0
1/15         0        0          0           0     0
1/16         0        0          0           0     0
1/17         0        0          0           0     0
1/18         0        0          0           0     0
1/19         0        0          0           0     0
1/20         0        0          0           0     0
1/21         0        0          0           0     0
1/22         0        0          0           0     0
1/23        27      819          0           3     0
1/24         0        0          0           0     0
Console#
```

show interfaces switchport

Use this command to display the administrative and operational status of specified interfaces.

Syntax

show interfaces switchport [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

 © 2004 Foundry Networks, Inc.

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. The items displayed by this command include:

- **Broadcast threshold** – Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 4-114).
- **Lacp status** – Shows if Link Aggregation Control Protocol has been enabled or disabled (page 4-182).
- **Dual-mode** – Indicates if Dual Mode has been enabled.
- **VLAN membership mode** – Indicates membership mode as Trunk or Hybrid (page 4-144).
- **Ingress rule** – Shows if ingress filtering is enabled or disabled (page 4-145).
- **Acceptable frame type** – Shows if acceptable VLAN frames include all types or tagged frames only (page 4-145).
- **Native VLAN** – Indicates the default Port VLAN ID (page 4-146).
- **Priority for untagged traffic** – Indicates the default priority for untagged frames (page 4-164).
- **Gvrp status** – Shows if GARP VLAN Registration Protocol is enabled or disabled (page 4-154).
- **Allowed Vlan** – Shows the VLANs this interface has joined, where "(u)" indicates untagged and "(t)" indicates tagged (page 4-147).
- **Forbidden Vlan** – Shows the VLANs this interface can not dynamically join via GVRP (page 4-148).

Example

This example shows the configuration setting for Ethernet port 15.

```
Console#show interfaces switchport ethernet 1/15
Information of Eth 1/23
 Broadcast threshold: Enabled, 500 packets/second
 Lacp status: Disabled
 Dual-mode: 0
 Ingress rate limit: disable,1000M bits per second
 Egress rate limit: disable,1000M bits per second
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Disabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:
Console#
```

Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Command	Function	Mode	Page
mac-address-table static	Maps a static address to a port in a VLAN	GC	4-121
show mac-address-table	Displays entries in the forwarding database	PE	4-122
clear mac-address-table dynamic	Removes any learned entries from the forwarding database	PE	4-123
mac-address-table aging-time	Sets the aging time of the address table	GC	4-123
show mac-address-table aging-time	Showsthe aging time for the address table	PE	4-123

mac-address-table static

Use this command to map a static address to a port in a VLAN. Use the **no** form to remove an address.

Syntax

mac-address-table static *mac-address interface* **vlan** *vlan-id* [*action*]
no mac-address-table static *mac-address* **vlan** *vlan-id*

- *mac-address* - MAC address.
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-4)
- *vlan-id* - VLAN ID (Range: 1-4094)
- *action* -
  - **delete-on-reset** - Assignment lasts until switch is reset.
  - **permanent** - Assignment is permanent.

Default Setting

No static addresses are defined. The default mode is **permanent**.

Command Mode

Global Configuration

Command Usage

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses will not be removed from the address table when a given interface link is down.

© 2004 Foundry Networks, Inc.

- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de ethernet 1/1 vlan 1 delete-on-reset
Console(config)#
```

show mac-address-table

Use this command to view classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [**address** *mac-address* [*mask*]] [**interface** *interface*] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

- *mac-address* - MAC address.
- *mask* - Bits to match in the address.
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-4)
- *vlan-id* - VLAN ID (Range: 1-4094)
- **sort** - Sort by address, vlan or interface.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
  - Learned - dynamic address entries
  - Permanent - static entry
  - Delete-on-reset - static entry to be deleted when system is reset
- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit “0” means to match a bit and “1” means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means “any.”
- The maximum number of address entries is 8191.

 © 2004 Foundry Networks, Inc.

Example

```
Console#show mac-address-table
 Interface Mac Address        Vlan Type
 --------- -----------------  ---- -----------------
  Eth 1/ 1 00-e0-29-94-34-de   1   Delete-on-reset
Console#
```

clear mac-address-table dynamic

Use this command to remove any learned entries from the forwarding database and to clear the transmit and receive counts for any static or system configured entries.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear mac-address-table dynamic
Console#
```

mac-address-table aging-time

Use this command to set the aging time for entries in the address table. Use the **no** form to restore the default aging time.

Syntax

mac-address-table aging-time *seconds*
no mac-address-table aging-time

seconds - Time is number of seconds
(EdgeIron 4802CF, 2402CF, 24G-A and 48G: 0, or 10-1000000; EdgeIron 24G: 17-2184.)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

Example

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

show mac-address-table aging-time

Use this command to show the aging time for entries in the address table.

Default Setting

None

 © 2004 Foundry Networks, Inc.

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table aging-time
 Aging time: 300 sec.
Console#
```

Spanning Tree Commands

This section includes commands that configure the Spanning Tree Protocol (STP) for the overall switch, and commands that configure STP for the selected interface.

Command	Function	Mode	Page
spanning-tree	Enables the spanning tree protocol	GC	4-125
spanning-tree forward-time	Configures the spanning tree bridge forward time	GC	4-126
spanning-tree hello-time	Configures the spanning tree bridge hello time	GC	4-126
spanning-tree max-age	Configures the spanning tree bridge maximum age	GC	4-127
spanning-tree priority	Configures the spanning tree bridge priority	GC	4-127
spanning-tree path-cost method	Configures the path cost method for RSTP/MSTP	GC	4-128
spanning-tree transmission-limit	Configures the transmission limit for RSTP/MSTP	GC	4-128
spanning-tree spanning-disabled	Disables spanning tree for an interface	IC	4-129
spanning-tree mst-configuration	Changes to MSTP configuration mode	GC	4-130
mst vlan	Adds VLANs to a spanning tree instance	MST	4-130
mst priority	Configures the priority of a spanning tree instance	MST	4-131
name	Configures the name for the multiple spanning tree	MST	4-131
revision	Configures the revision number for the multiple spanning tree	MST	4-132
max-hops	Configures the maximum number of hops allowed in the region before a BPDU is discarded	MST	4-132
spanning-tree cost	Configures the spanning tree path cost of an interface	IC	4-133
spanning-tree port priority	Configures the spanning tree priority of an interface	IC	4-134
spanning-tree portfast	Sets an interface to fast forwarding	IC	4-134
spanning-tree edge-port	Enables fast forwarding for edge ports	IC	4-135
spanning-tree protocol-migration	Re-checks the appropriate BPDU format	PE	4-136
spanning-tree link-type	Configures the link type for RSTP/MSTP	IC	4-136
spanning-tree mst cost	Configures the path cost of an instance in the MST	IC	4-137

© 2004 Foundry Networks, Inc.

Command	Function	Mode	Page
spanning-tree mst port-priority	Configures the priority of an instance in the MST	IC	4-138
show spanning-tree	Shows the spanning tree configuration for the common spanning tree or for an instance within the multiple spanning tree	PE	4-137
show spanning-tree mst configuration	Shows the multiple spanning tree configuration	PE	4-139

Note: The **spanning-tree mode** command has been removed and replaced by RSTP mode for the global spanning tree and PVST-compliant mode for each VLAN. If the switch detects a device running STP it will automatically downgrade to STP. Presently the firmware does not support MSTP.

spanning-tree

Use this command to enable the Spanning Tree Protocol globally for this switch. Use the **no** form to disable it.

Syntax

spanning-tree
no spanning-tree

Default Setting

Spanning tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Protocol can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

The following example enables the Spanning Tree Protocol for this switch:

```
Console(config)#spanning-tree
Console(config)#
```


© 2004 Foundry Networks, Inc.

spanning-tree forward-time

Use this command to configure the SpanningTree bridge forward time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree forward-time *seconds*
no spanning-tree forward-time

seconds - Time in seconds. (Range: 4-30 seconds)
The minimum value is the higher of 4 or [(max-age / 2) + 1].

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

Use this command to configure the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree hello-time *time*
no spanning-tree hello-time

time - Time in seconds. (Range: 1-10 seconds)
The maximum value is the lower of 10 or [(max-age / 2) -1].

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

 © 2004 Foundry Networks, Inc.

spanning-tree max-age

Use this command to configure the spanning tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree max-age *seconds*
no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)
The minimum value is the higher of 6 or [2 x (hello-time + 1)].
The maximum value is the lower of 40 or [2 x (forward-time - 1)].

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

spanning-tree priority

Use this command to configure the spanning tree priority globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree priority *priority*
no spanning-tree priority

priority - Priority of the bridge.
(Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

© 2004 Foundry Networks, Inc.

Example

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

spanning-tree pathcost method

Use this command to configure the path cost method used for the Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree pathcost method {**long** | **short**}
no spanning-tree pathcost method

- **long** - Specifies 32-bit based values that range from 1-200,000,000.
- **short** - Specifies 16-bit based values that range from 1-65535.

Default Setting

short method

Command Mode

Global Configuration

Command Usage

The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost (page 4-133) takes precedence over port priority (page 4-134).

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree transmission-limit

Use this command to configure the minimum interval between the transmission of consecutive RSTP/MSTP BPDUs. Use the **no** form to restore the default.

Syntax

spanning-tree transmission-limit *count*
no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

Default Setting

3

Command Mode

Global Configuration

Command Usage

This command limit the maximum transmission rate for BPDUs.

 © 2004 Foundry Networks, Inc.

Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

spanning-tree spanning-disabled

This command disables the spanning tree algorithm for the specified interface. Use the **no** form to reenable the spanning tree algorithm for the specified interface.

Syntax

[no] spanning-tree spanning-disabled

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

This example disables the spanning tree algorithm for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

Multiple Spanning Tree

Notes: 1. All settings for MSTP are applicable to PVST configuration.

2. The **spanning-tree mode** command has been removed and replaced by RSTP mode for the global spanning tree and PVST-compliant mode for each VLAN. If the switch detects a device running STP it will automatically downgrade to STP. Presently the firmware does not support MSTP.

spanning-tree mst-configuration

Use this command to change to Multiple Spanning Tree (MST) configuration mode.

Default Setting

- No VLANs are mapped to any MST instance.
- The region name is set the switch's MAC address.

Command Mode

Global Configuration

Example

```
Console(config)#spanning-tree mst-configuration
Console(config-mstp)#
```


© 2004 Foundry Networks, Inc.

spanning-tree mst-configuration

Use this command to change to Multiple Spanning Tree (MST) configuration mode.

Default Setting

- No VLANs are mapped to any MST instance.
- The region name is undefined.

Command Mode

Global Configuration

Example

```
Console(config)#spanning-tree mst-configuration
Console(config-mst)#
```

Related Commands

mst vlan (4-130)
mst priority (4-131)
name (4-131)
revision (4-132)
max-hops (4-132)

mst vlan

Use this command to add VLANs to a Spanning Tree instance. Use the **no** form to remove the specified VLANs. Using the **no** form without any VLAN parameters to remove all VLANs.

Syntax

mst *instance_id* **vlan** *vlan-range*
no mst *instance_id* [**vlan** *vlan-range*]

- *instance_id* - Instance identifier of the spanning tree. (Range: 0-63)
- *vlan-range* - Range of VLANs. (Range: 1-4094)

Default Setting

none

Command Mode

MST Configuration

Command Usage

- Use this command to group VLANs into spanning tree instances. MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.
- By default all VLANs are assigned to the Internal Spanning Tree (MSTI 0) that connects all bridges and LANs within the MST region. This switch supports up to 65 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region (page) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, and connects all regions to the Common Spanning Tree.

 © 2004 Foundry Networks, Inc.

Example

```
Console(config-mst)#mst 1 vlan 2-5
Console(config-mst)#
```

mst priority

Use this command to configure the priority of a spanning tree instance. Use the **no** form to restore the default.

Syntax

mst *instance_id* **priority** *priority*
no mst *instance_id* **priority**

- *instance_id* - Instance identifier of the spanning tree. (Range: 0-64)
- *priority* - Priority of the a spanning tree instance.
  (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

MST Configuration

Command Usage

- MST priority is used in selecting the root bridge and alternate bridge of the specified instance. The device with the highest priority (i.e., lowest numerical value) becomes the MSTI root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- You can set this switch to act as the MSTI root device by specifying a priority of 0, or as the MSTI alternate device by specifying a priority of 16384.

Example

```
Console(config-mst)#mst 1 priority 4096
Console(config-mst)#
```

name

Use this command to configure the name for the multiple spanning tree region in which this switch is located. Use the **no** form to clear the name.

Syntax

name *name*

name - Name of the spanning tree.

Default Setting

none

Command Mode

MST Configuration

© 2004 Foundry Networks, Inc.

Command Usage

The MST region name and revision number (page) are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

Example

```
Console(config-mst)#name R&D
Console(config-mst)#
```

Related Commands

revision

revision

Use this command to configure the revision number for this multiple spanning tree configuration of this switch. Use the **no** form to restore the default.

Syntax

revision *number*

number - Revision number of the spanning tree. (Range: 0-65535)

Default Setting

0

Command Mode

MST Configuration

Command Usage

The MST region name (page) and revision number are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

Example

```
Console(config-mst)#revision 1
Console(config-mst)#
```

Related Commands

name

max-hops

Use this command to configure the maximum number of hops in the region before a BPDU is discarded. Use the **no** form to restore the default.

Syntax

max-hops hop-number

hop-number - Maximum hop number for multiple spanning tree. (Range: 1-40)

Default Setting

20

Command Mode

MST Configuration

 © 2004 Foundry Networks, Inc.

Command Usage

A MSTI region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside a MSTI region is never changed. However, each spanning tree instance within a region, and the internal spanning tree (IST) that connects these instances use a hop count to specify the maximum number of bridges that will propagate a BPDU. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

Example

```
Console(config-mst)#max-hops 30
Console(config-mst)#
```

spanning-tree cost

Use this command to configure the spanning tree path cost for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree cost *cost*
no spanning-tree cost

cost - The path cost for the interface.
(Range – 1-200,000,000)
The recommended range is -
- Ethernet: 200,000-20,000,000
- Fast Ethernet: 20,000-2,000,000
- Gigabit Ethernet: 2,000-200,000

Default Setting

- Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet – full duplex: 10,000; trunk: 5,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This parameter is used by the Spanning-Tree Protocol to determine the best path between devices. Therefore, lower values should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.
- Path cost takes precedence over interface priority.
- When the Spanning-Tree pathcost method is set to **short**, the maximum value for path cost is 65,535.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

Related Commands

spanning-tree port-priority (4-134)

© 2004 Foundry Networks, Inc.

spanning-tree port-priority

Use this command to configure the priority for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree port-priority *priority*
no spanning-tree port-priority

priority - The priority for an interface. (Range: 0-240, in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of an interface in the spanning tree. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
Console(config-if)#
```

Related Commands

spanning-tree cost (4-133)

spanning-tree portfast

Use this command to set an interface to fast forwarding. Use the **no** form to disable fast forwarding.

Syntax

spanning-tree portfast
no spanning-tree portfast

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used to enable/disable the fast spanning tree mode for the selected interface. In this mode, interfaces skip the Learning state and proceed straight to Forwarding.

 © 2004 Foundry Networks, Inc.

- Since end-nodes cannot cause forwarding loops, they can be passed through the spanning tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STP related timeout problems. (Remember that fast forwarding should only be enabled for ports connected to a LAN segment that is at the end of a bridged LAN, or for an end-node device.)
- This command is the same as **spanning-tree edge-port**, and is only included for backward compatibility with earlier products. Note that this command may be removed for future software versions.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree portfast
Console(config-if)#
```

Related Commands

spanning-tree edge-port (4-135)

spanning-tree edge-port

Use this command to specify an interface as an edge port. Use the **no** form to restore the default.

Syntax

spanning-tree edge-port
no spanning-tree edge-port

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- You can enable this option if an interface is attached to a LAN segment that is at the end of bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STP-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- This command has the same effect as the **spanning-tree portfast** command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

Related Commands

spanning-tree portfast (4-134)

© 2004 Foundry Networks, Inc.

spanning-tree protocol-migration

Use this command to re-check the appropriate BPDU format to send on the selected interface.

Syntax

spanning-tree protocol-migration *interface*

interface

- **ethernet** *unit*/*port-number*
  - *unit* - This is device 1.
  - *port-number*
- **port-channel** *channel-id* (Range: 1-6)

Command Mode

Privileged Exec

Command Usage

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the **spanning-tree protocol-migration** command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree protocol-migration
Console(config-if)#
```

spanning-tree link-type

Use this command to configure the link type for the Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree link-type {**auto** | **point-to-point** | **shared**}
no spanning-tree link-type

- **auto** - Automatically derived from the duplex mode setting.
- **point-to-point** - Point-to-point link.
- **shared** - Shared medium.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.

 © 2004 Foundry Networks, Inc.

- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden. Since MSTP is an extension of RSTP, this same restriction applies.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
Console(config-if)#
```

spanning-tree mst cost

Use this command to configure the path cost on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree mst *instance_id* **cost** *cost*
no spanning-tree mst *instance_id* **cost**

- *instance_id* - Instance identifier of the spanning tree. (Range: 1-4094, no leading zeroes)
- *cost* - Path cost for an interface. (Range: 1-200,000,000) The recommended range is -
  - Ethernet: 200,000-20,000,000
  - Fast Ethernet: 20,000-2,000,000
  - Gigabit Ethernet: 2,000-200,000

Default Setting

- Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet – full duplex: 10,000; trunk: 5,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Each spanning-tree instance is associated with a unique set of VLAN IDs.
- This command is used by the multiple spanning-tree algorithm to determine the best path between devices. Therefore, lower values should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.
- Path cost takes precedence over interface priority.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

Related Commands

spanning-tree mst port-priority (4-138)

© 2004 Foundry Networks, Inc.

spanning-tree mst port-priority

Use this command to configure the interface priority on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree mst *instance_id* **port-priority** *priority*
no spanning-tree mst *instance_id* **port-priority**

- *instance_id* - Instance identifier of the spanning tree. (Range: 1-4094, no leading zeroes)
- *priority* - Priority for an interface. (Range: 0-240 in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of an interface in the multiple spanning-tree. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

Related Commands

spanning-tree mst cost (4-137)

show spanning-tree

Use this command to show the configuration for the common spanning tree (CST) or for an instance within the multiple spanning tree (MSTI).

Syntax

show spanning-tree [*interface* | **mst** *instance_id*]

- *interface*
  - **ethernet** *unit*/*port-number*
    - *unit* - This is device 1.
    - *port-number*
  - **port-channel** *channel-id* (Range: 1-6)
- *instance_id* - Instance identifier of the multiple spanning tree. (Range: 0-64, no leading zeroes)

Default Setting

None

 © 2004 Foundry Networks, Inc.

Command Mode

Privileged Exec

Command Usage

- Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the Common spanning tree (CST) and for every interface in the tree.
- Use the **show spanning-tree** *interface* command to display the spanning tree configuration for an interface within the Common spanning tree (CST).
- For a description of the items displayed under “Spanning-tree information,” see “STP Configuration” on page 3-77. For a description of the items displayed for specific interfaces, see “STP Port and Trunk Information” on page 3-81.
- Use the **show spanning-tree mst** *instance_id* command to display the spanning tree configuration for an instance within the Multiple Spanning Tree (MST).

Example

```
Console#show spanning-tree
Spanning-tree information
---------------------------------------------------------------------
 Spanning tree mode               :RSTP
 Spanning tree enable/disable     :enable
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Designated Root                  :32768.000011112222
 Current root port                :0
 Current root cost                :0
 Number of topology changes       :1
 Last topology changes time (sec.):25067
 Transmission limit               :3
 Path Cost Method                 :long
---------------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------------
 Admin status         : enable
 Role                 : disable
 State                : discarding
 Path cost            : 10000
 Priority             : 128
 Designated cost      : 0
 Designated port      : 128.1
 Designated root      : 32768.000011112222
 Designated bridge    : 32768.000011112222
 Fast forwarding      : disable
 Forward transitions  : 0
 Admin edge port      : disable
 Oper edge port       : disable
 Admin Link type      : auto
 Oper Link type       : point-to-point
.
.
.
Console#
```

show spanning-tree mst configuration

Use this command to show the configuration of the multiple spanning tree.

Syntax

show spanning-tree mst configuration

Command Mode

Privileged Exec

 © 2004 Foundry Networks, Inc.

Example

```
Console#show spanning-tree mst configuration
Mstp Configuration Information
-------------------------------------------------------------
 Instance Vlans
-------------------------------------------------------------
     0    1-4094
     1    1
     2    2
     3    3
     4    4
     5    5
.
.
.

    60    60
    61    61
    62    62
    63    63
    64    64
Console#
```

VLAN Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

Command	Function	Mode	Page
Edit VLAN Groups			
vlan	Configures a VLAN, including VID, name and state	GC	4-141
untagged ethernet	Assign a port as an untagged member of a port-based VLAN	VC	4-142
tagged ethernet	Assigns a port as a tagged member of a port-based VLAN	VC	4-142
dual-mode	Configures a tagged port to transmit and receive both tagged and untagged frames	IC	4-143
Configure VLAN Interfaces			
interface vlan	Enters interface configuration mode for specified VLAN	IC	4-144
switchport mode	Configures VLAN membership mode for an interface	IC	4-144
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC	4-145
swicthport ingress-filtering	Enables ingress filtering on an interface	IC	4-145
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC	4-146
switchport allowed vlan	Configures the VLANs associated with an interface	IC	4-147
switchport gvrp	Enables GVRP for an interface	IC	4-154
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	4-148

 © 2004 Foundry Networks, Inc.

Command	Function	Mode	Page
Display VLAN Information			
show vlan	Shows VLAN information	NE, PE	4-148
show interfaces status vlan	Displays status for the specified VLAN interface	NE, PE	4-119
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	4-119

vlan

Use this command to create VLANs and enter VLAN configuration mode. Use the **no** form to delete a VLAN.

Syntax

vlan *vlan-id* [**by port** | **name** *vlan-name*]
no vlan *vlan-id*

- *vlan-id* - ID of configured VLAN. (Range: 1-4094, no leading zeroes)
- **by port** - Forces the VLAN to be port based.
- **name** - Keyword to be followed by the VLAN name.
  - *vlan-name* - ASCII string from 1 to 16 characters.

Note: The maximum length of a VLAN name is 16 characters (the same as RFC2674 MIB definition). When a VLAN name is set through the ifAlias object (RFC2863 MIB), up to 64 characters can be used, but the name is always truncated to 16 characters, because both refer to the same database. The maximum lengths for all other names (such as ports and trunks) are 64 characters.

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

Global Configuration

Command Usage

- Use the VLAN command mode to add, change and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the **show vlan** command.
- When **no vlan** *vlan-id* is used, the VLAN is deleted.
- You can configure up to 255 VLANs on the switch.

Example

The following example adds a VLAN, using vlan-id 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan 105 name RD5
Console(config-vlan-105)#
```

Related Commands

show vlan (4-148)

© 2004 Foundry Networks, Inc.

untagged ethernet

Use this command to assign ports as untagged members of a port-based VLAN. Use the **no** form to remove ports from a port-based VLAN.

Syntax

untagged ethernet *interface* [**to** *interface*]
no untagged ethernet *interface* [**to** *interface*]

- *interface* - Specifies a port number, or the start or end of a port range, to assign to the VLAN.
  - *unit*/*port*
    - *unit* - This is device 1.
    - *port* - Port number.
- **to** - Specifies the end of a port number range.

Default Setting

None

Command Mode

VLAN Configuration

Example

The following example shows how to assign switch ports 1 to 8 as untagged members of VLAN 222.

```
Console(config)#vlan 222 by port
Console(config-vlan-222)#untagged ethernet 1/1 to 1/8
Console(config-if)#
```

Related Commands

vlan (4-141)
tagged ethernet (4-142)
dual mode (4-143)

tagged ethernet

Use this command to assign ports as tagged members of a port-based VLAN. Use the **no** form to remove ports from the port-based VLAN.

Syntax

tagged ethernet *interface* [**to** *interface*]
no tagged ethernet *interface* [**to** *interface*]

- *interface* - Specifies a port number, or the start or end of a port range, to assign to the VLAN.
  - *unit*/*port*
    - *unit* - This is device 1.
    - *port* - Port number.
- **to** - Specifies the end of a port number range.

Default Setting

None

Command Mode

VLAN Configuration

© 2004 Foundry Networks, Inc.

Example

The following example shows how to assign port 5 as a tagged member of VLAN 222.

```
Console(config)#vlan 222 by port
Console(config-vlan-222)#tagged ethernet 1/5
Console(config-if)#
```

dual-mode

Use this command to enable a tagged VLAN port to accept and transmit both tagged and untagged traffic. Use the **no** form to restore the default setting.

Syntax

dual-mode [*vlan_id*]
no dual-mode

- *vlan_id* - Specifies the default VLAN ID for the port. (Range: 1-4094, no leading zeroes).

Default Setting

Disabled

Command Usage

Configuring a tagged port as a dual-mode port allows it to accept and transmit both tagged traffic and untagged traffic at the same time. A dual-mode port transmits only untagged traffic on its default VLAN (that is either VLAN 1, or a user specified VLAN ID), and only tagged traffic on all other VLANs.

Command Mode

Interface Configuration

Example

The following example shows how to enable dual-mode on port 5 and set its default VLAN ID to 10.

```
Console(config)#vlan 10 by port
Console(config-vlan-10)#untagged ethernet 1/1
Console(config)#vlan 222 by port
Console(config-vlan-222)#tagged ethernet 1/5
Console(config)#interface ethernet 1/5
Console(config-if)#dual-mode 10
Console(config-if)#
```

Related Commands

vlan (4-141)
tagged ethernet (4-142)
untagged ethernet (4-142)

© 2004 Foundry Networks, Inc.

Configuring VLAN Interfaces

interface vlan

Use this command to enter interface configuration mode for VLANs, and configure a physical interface.

Syntax

interface vlan *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)

Default Setting

None

Command Mode

Global Configuration

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

switchport mode

Use this command to configure the VLAN membership mode for a port. Use the **no** form to restore the default.

Syntax

switchport mode {**trunk** | **hybrid**}
no switchport mode

- **trunk** - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e.,associated with the PVID) are also transmitted as tagged frames.
- **hybrid** - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

Default Setting

All ports are in hybrid mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```


© 2004 Foundry Networks, Inc.

Related Commands

switchport acceptable-frame-types (4-145)

switchport acceptable-frame-types

Use this command to configure the acceptable frame types for a port. Use the **no** form to restore the default.

Syntax

switchport acceptable-frame-types {**all** | **tagged**}
no switchport acceptable-frame-types

- **all** - The port passes all frames, tagged or untagged.
- **tagged** - The port only passes tagged frames.

Default Setting

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Example

The following example shows how to restrict the traffic passed on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

Related Commands

switchport mode (4-144)

switchport ingress-filtering

Use this command to enable ingress filtering for an interface. Use the **no** form to restore the default.

Syntax

switchport ingress-filtering
no switchport ingress-filtering

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

 © 2004 Foundry Networks, Inc.

Command Usage

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport native vlan

Use this command to configure the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

Syntax

switchport native vlan *vlan-id*
no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4094, no leading zeroes)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

 © 2004 Foundry Networks, Inc.

switchport allowed vlan

Use this command to configure VLAN groups on the selected interface. Use the **no** form to restore the default.

Syntax

switchport allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] | **remove** *vlan-list*}
no switchport allowed vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094)

Default Setting

All ports are assigned to VLAN 1 by default.
The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If switchport mode is set to **trunk**, then you can only assign an interface to VLAN groups as a tagged member.
- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.
- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 2,5,6 tagged
Console(config-if)#
```


© 2004 Foundry Networks, Inc.

switchport forbidden vlan

Use this command to configure forbidden VLANs. Use the **no** form to remove the list of forbidden VLANs.

Syntax

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}
no switchport forbidden vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094)

Default Setting

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

Example

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

show vlan

Use this command to show VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- **id** - Keyword to be followed by the VLAN ID.
  - *vlan-id* - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  - *vlan-name* - ASCII string from 1 to 32 characters.

Default Setting

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

 © 2004 Foundry Networks, Inc.

Example

The following example shows how to display information for VLAN 33:

```
Console#show vlan id 1
VLAN Type    Name             Status    Ports/Channel groups
---- ------- ---------------- --------- -------------------------------------
33  Static Blue            Active  Eth1/ 2 Eth1/ 3  Eth1/ 6 Eth1/ 7
                                   Eth1/ 9 Eth1/ 10  Eth1/ 11 Eth1/ 12
Console#
```

Private VLAN Commands

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. This switch supports two types of private VLAN ports: promiscuous, and community ports. A promiscuous port can communicate with all interfaces within a private VLAN. Community ports can only communicate with other ports in their own community VLAN, and with their designated promiscuous ports. This section describes commands used to conigure private VLANs.

Command	Function	Mode	Page
Edit Private VLAN Groups			
private-vlan	Adds or deletes primary and secondary VLANs	VC	4-150
private-vlan association	Associates a secondary VLAN with a primary VLAN	VC	4-150
Configure Private VLAN Interfaces			
switchport mode private-vlan	Sets an interface to host mode or promiscuous mode	IC	4-151
switchport private-vlan host-association	Associates an interface with a secondary VLAN	IC	4-152
switchport private-vlan mapping	Maps an interface to a primary VLAN	IC	4-152
Display Private VLAN Information			
show vlan private-vlan	Shows private VLAN information	NE, PE	4-153

To configure private VLANs, follow these steps:

1. Use the **private-vlan** command to designate one or more community VLANs and the primary VLAN that will channel traffic outside the community groups.
2. Use the **private-vlan association** command to map the secondary (i.e., community) VLAN(s) to the primary VLAN.
3. Use the **switchport mode private-vlan** command to configure ports as promiscuous (i.e., having access to all ports in the primary VLAN) or host (i.e., having access restricted to community VLAN members, and channeling all other traffic through a promiscuous port).
4. Use the **switchport private-vlan host-association** command to assign a port to a secondary VLAN.
5. Use the **switchport private-vlan mapping** command to assign a port to a primary VLAN.
6. Use the **show vlan private-vlan** command to verify your configuration settings.

 © 2004 Foundry Networks, Inc.

Editing Private VLAN Groups

private-vlan

Use this command to create a primary or secondary (i.e., community) private VLAN. Use the **no** form to remove the specified private VLAN.

Syntax

private-vlan *vlan-id* {**community** | **primary**}
no private-vlan *vlan-id*

- *vlan-id* - ID of private VLAN. (Range: 1-4093, no leading zeroes).
- **community** – Specifies a community VLAN.
- **primary** – Specifies a primary VLAN.

Default Setting

None

Command Mode

VLAN Configuration

Command Usage

- Private VLANs are used to restrict traffic to ports within the same VLAN "community," and channel traffic passing outside the community through promiscuous ports that have been mapped to the associated "primary" VLAN.
- Port membership for private VLANs is static. Once a port has been assigned to a private VLAN, it cannot be dynamically moved to another VLAN via GVRP.
- Private VLAN ports cannot be set to trunked mode. (See "switchport mode" on page 4-144.)

Example

```
Console(config)#vlan database
Console(config-vlan)#private-vlan 2 primary
Console(config-vlan)#private-vlan 3 community
Console(config)#
```

private vlan association

Use this command to associate a primary VLAN with a secondary (i.e., community) VLAN. Use the **no** form to remove all associations for the specified primary VLAN.

Syntax

private-vlan *primary-vlan-id* **association** {*secondary-vlan-id* | **add** *secondary-vlan-id* | **remove** *secondary-vlan-id*}

no private-vlan *primary-vlan-id* **association**

- *primary-vlan-id* - ID of primary VLAN.
  (Range: 2-4094, no leading zeroes).
- *secondary-vlan-id* - ID of secondary (i.e, community) VLAN. (Range: 2-4094, no leading zeroes).

Default Setting

None

 © 2004 Foundry Networks, Inc.

Command Mode

VLAN Configuration

Command Usage

Secondary VLANs provide security for group members. The associated primary VLAN provides a common interface for access to other network resources within the primary VLAN (e.g., servers configured with promiscuous ports) and to resources outside of the primary VLAN (via promiscuous ports).

Example

```
Console(config-vlan)#private-vlan 2 association 3
Console(config)#
```

Configuring Private VLAN Interfaces

switchport mode private-vlan

Use this command to set the private VLAN mode for an interface. Use the **no** form to restore the default setting.

Syntax

switchport mode private-vlan {**host** | **promiscuous**}
no switchport mode private-vlan

- **host** – This port type can communicate with all other host ports assigned to the same secondary VLAN. All communications outside of this VLAN must pass through a promiscuous port in the associated primary VLAN.
- **promiscuous** – This port type can communicate with all other promiscuous ports in the same primary VLAN, as well as with all the ports in the associated secondary VLANs.

Default Setting

Normal VLAN

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Promiscuous ports assigned to a primary VLAN can communicate with all other promiscuous ports in the same VLAN, as well as with all the ports in the associated secondary VLANs.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport mode private-vlan promiscuous
Console(config)#exit
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan host
Console(config)#
```


© 2004 Foundry Networks, Inc.

switchport private-vlan host-association

Use this command to associate an interface with a secondary VLAN. Use the **no** form to remove this association.

Syntax

switchport private-vlan host-association *secondary-vlan-id*
no switchport private-vlan host-association

- *secondary-vlan-id* – ID of secondary (i.e, community) VLAN. (Range: 1-4093, no leading zeroes).

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

All ports assigned to a secondary (i.e., community) VLAN can pass traffic between group members, but must communicate with resources outside of the group via a promiscuous port.

Example

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan host-association 3
Console(config)#
```

switchport private-vlan mapping

Use this command to map an interface to a primary VLAN. Use the **no** form to remove this mapping.

Syntax

switchport private-vlan mapping *primary-vlan-id*
no switchport private-vlan mapping

primary-vlan-id – ID of primary VLAN. (Range: 1-4093, no leading zeroes).

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Promiscuous ports assigned to a primary VLAN can communicate with any other promiscuous ports in the same VLAN, and with the group members within any associated secondary VLANs.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport private-vlan mapping 2
Console(config)#
```

 © 2004 Foundry Networks, Inc.

Displaying Private VLAN Information

show vlan private-vlan

Use this command to show the private VLAN configuration settings on this switch.

Syntax

show vlan private-vlan [**community** | **primary**]

- **community** – Displays all community VLANs, along with their associate primary VLAN and assigned host interfaces.
- **primary** – Displays all primary VLANs, along with any assigned promiscuous interfaces.

Default Setting

None

Command Mode

Privileged Executive

Example

```
Console#show vlan private-vlan
Primary   Secondary       Type       Interfaces
--------  -----------  ----------  ------------------------------
     5                 primary     Eth1/ 3
     5         6       community   Eth1/ 4 Eth1/ 5
Console#
```

GVRP and Bridge Extension Commands

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.This section describes how to display default configuration settings for the Bridge Extension MIB.

Note: Under the following condition, GVRP does not leave and join dynamically. In LAB testing, tagged frames transmitted at wire speed, dynamically changing the VLAN tag information from VLAN ID 1 to 128, results in GVRP failing after 10 to 20 minutes.

Command	Function	Mode	Page
Interface Commands			
switchport gvrp	Enables GVRP for an interface	IC	4-154
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	4-148
show gvrp configuration	Displays GVRP configuration for selected interface	NE, PE	4-154
garp timer	Sets the GARP timer for the selected function	IC	4-155
show garp timer	Shows the GARP timer for the selected function	NE, PE	4-156

© 2004 Foundry Networks, Inc.

Command	Function	Mode	Page
Global Commands			
bridge-ext gvrp	Enables GVRP globally for the switch	GC	4-156
show bridge-ext	Shows bridge extension configuration	PE	4-157

switchport gvrp

Use this command to enable GVRP for a port. Use the **no** form to disable it.

Syntax

switchport gvrp
no switchport gvrp

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

show gvrp configuration

Use this command to show if GVRP is enabled.

Syntax

show gvrp configuration [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows both global and interface-specific configuration.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
 Gvrp configuration: Disabled
Console#
```


© 2004 Foundry Networks, Inc.

garp timer

Use this command to set the values for the join, leave and leaveall timers. Use the **no** form to restore the timers' default values.

Syntax

garp timer {**join** | **leave** | **leaveall**} *timer_value*
no garp timer {**join** | **leave** | **leaveall**}

- {**join** | **leave** | **leaveall**} - Which timer to set.
- *timer_value* - Value of timer.
  Ranges:
  join: 20-1000 centiseconds
  leave: 60-3000 centiseconds
  leaveall: 500-18000 centiseconds

Default Setting

- join: 20 centiseconds
- leave: 60 centiseconds
- leaveall: 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
- Timer values are applied to GVRP for all the ports on all VLANs.
- Timer values must meet the following restrictions:
  leave >= (2 x join)
  leaveall > leave

Note: Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP will not operate successfully.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

Related Commands

show garp timer (4-156)

© 2004 Foundry Networks, Inc.

show garp timer

Use this command to show the GARP timers for the selected interface.

Syntax

show garp timer [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows all GARP timers.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
 Join timer: 20 centiseconds
 Leave timer: 60 centiseconds
 Leaveall timer: 1000 centiseconds

Console#
```

Related Commands

garp timer (4-155)

bridge-ext gvrp

Use this command to enable GVRP. Use the **no** form to disable it.

Syntax

bridge-ext gvrp
no bridge-ext gvrp

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Example

```
Console(config)#bridge-ext gvrp
Console(config)#
```

 © 2004 Foundry Networks, Inc.

show bridge-ext

Use this command to show the configuration for bridge extension commands.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See “Displaying Basic VLAN Information” on page 3-92 and “Port Configuration” on page 3-52 for a description of the displayed items.

Example

```
Console#show bridge-ext
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Disabled
 GMRP: Disabled
Console#
```

IGMP Snooping Commands

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Command	Function	Mode	Page
Basic IGMP Commands			
ip igmp snooping	Enables IGMP snooping	GC	4-158
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC	4-158
ip igmp snooping version	Configures the IGMP version for snooping	GC	4-159
show ip igmp snooping	Shows the IGMP snooping configuration	PE	4-159
show bridge multicast	Shows the IGMP snooping MAC multicast list	PE	4-160
IGMP Querier Commands			
ip igmp snooping querier	Allows this device to act as the querier for IGMP snooping	GC	4-160
ip igmp snooping query-count	Configures the query count	GC	4-161
ip igmp snooping query-interval	Configures the query interval	GC	4-161
ip igmp snooping query-max-response-time	Configures the report delay	GC	4-162

© 2004 Foundry Networks, Inc.

Command	Function	Mode	Page
ip igmp snooping router-port-expire-time	Configures the query timeout	GC	4-163
Multicast Router Commands			
ip igmp snooping vlan mrouter	Adds a multicast router port	GC	4-163
show ip igmp snooping mrouter	Shows multicast router ports	PE	4-164

Basic IGMP Commands

ip igmp snooping

Use this command to enable IGMP snooping on this switch. Use the **no** form to disable it.

Syntax

ip igmp snooping
no ip igmp snooping

Default Setting

Enabled

Command Mode

Global Configuration

Example

The following example enables IGMP snooping.

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping vlan static

Use this command to add a port to a multicast group. Use the no form to remove the port.

Syntax

ip igmp snooping vlan *vlan-id* **static** *ip-address interface*
no ip igmp snooping vlan vlan-id static *ip-address interface*

- *vlan-id* - VLAN ID (Range: 1-4094)
- *ip-address* - IP address for multicast group
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Global Configuration

© 2004 Foundry Networks, Inc.

Example

The following shows how to statically configure a multicast group on a port:

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

ip igmp snooping version

Use this command to configure the IGMP snooping version. Use the **no** form to restore the default.

Syntax

ip igmp snooping version {**1** | **2**}
no ip igmp snooping version

- **1** - IGMP Version 1
- **2** - IGMP Version 2

Default Setting

IGMP Version 2

Command Mode

Global Configuration

Command Usage

- All systems on the subnet must support the same version. If there are legacy devices in your network that only support Version 1, you will also have to configure this switch to use Version 1.
- Some commands are only enabled for IGMPv2, including **ip igmp query-max-response-time** and **ip igmp router-port-expire-time**.

Example

The following configures the switch to use IGMP Version 1:

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

show ip igmp snooping

Use this command to show the IGMP snooping configuration.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See “Configuring IGMP Parameters” on page 3-115 for a description of the displayed items.

 © 2004 Foundry Networks, Inc.

Example

The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
 Service status: Enabled
 Querier status: Enabled
 Query count: 2
 Query interval: 125 sec
 Query max response time: 10 sec
 Query time-out: 300 sec
 IGMP snooping version: Version 2
Console#
```

show mac-address-table multicast

Use this command to show known multicast addresses.

Syntax

show mac-address-table multicast [**vlan** *vlan-id*] [**user** | **igmp-snooping**]

- *vlan-id* - VLAN ID (1 to 4094)
- **user** - Display only the user-configured multicast entries.
- **igmp-snooping** - Display only entries learned through IGMP snooping.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Member types displayed include IGMP or USER, depending on selected options.

Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN    M'cast IP addr.  Member ports   Type
 ----    ---------------  ------------   -------
  1      224.1.2.3        Eth1/11        IGMP
Console#
```

IGMP Querier Commands

ip igmp snooping querier

Use this command to enable the switch as an IGMP snooping querier. Use the **no** form to disable it.

Syntax

ip igmp snooping querier
no ip igmp snooping querier

Default Setting

Enabled

Command Mode

Global Configuration

 © 2004 Foundry Networks, Inc.

Command Usage

If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping query-count

Use this command to configure the query count. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-count *count*
no ip igmp snooping query-count

count - The maximum number of queries issued for which there has been no response before the switch takes action to solicit reports. (Range: 2-10)

Default Setting

2 times

Command Mode

Global Configuration

Command Usage

The query count defines how long the querier waits for a response from a multicast client before taking action. If a querier has sent a number of queries defined by this command, but a client has not responded, a countdown timer is started using the time defined by **ip igmp snooping query-max-response-time**. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

ip igmp snooping query-interval

Use this command to configure the snooping query interval. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-interval *seconds*
no ip igmp snooping query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 60-125)

Default Setting

125 seconds

© 2004 Foundry Networks, Inc.

Command Mode

Global Configuration

Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

ip igmp snooping query-max-response-time

Use this command to configure the snooping report delay. Use the **no** form of this command to restore the default.

Syntax

ip igmp snooping query-max-response-time *seconds*
no ip igmp snooping query-max-response-time

seconds - The report delay advertised in IGMP queries. (Range: 5-30)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

- The switch must be using IGMPv2 for this command to take effect.
- This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the **ip igmp snooping query-count**, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the maximum response time to 20 seconds.

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

Related Commands

ip igmp snooping version (4-159)

 © 2004 Foundry Networks, Inc.

ip igmp snooping router-port-expire-time

Use this command to configure the snooping query-timeout. Use the **no** form of this command to restore the default.

Syntax

ip igmp snooping router-port-expire-time *seconds*
no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. (Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The switch must be using IGMPv2 for this command to take effect.

Example

The following shows how to configure the default timeout to 300 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 300
Console(config)#
```

Related Commands

ip igmp snooping version (4-159)

Multicast Router Commands

ip igmp snooping vlan mrouter

Use this command to statically configure a multicast router port. Use the **no** form to remove the configuration.

Syntax

ip igmp snooping vlan *vlan-id* **mrouter** *interface*
no ip igmp snooping vlan *vlan-id* **mrouter** *interface*

- *vlan-id* - VLAN ID (Range: 1-4094)
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

No static multicast router ports are configured.

© 2004 Foundry Networks, Inc.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your switch, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

Use this command to display information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static or Dynamic.

Example

The following shows the port in VLAN 1 that is attached to a multicast router:

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN     M'cast Router Ports  Type
 ----     -------------------  -------
  1        Eth 1/11            Static
  2        Eth 1/12            Dynamic
Console#
```

Priority Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, the relative weight of each queue, and the mapping of frame priority tags to the switch's priority queues.

 © 2004 Foundry Networks, Inc.

Command	Function	Mode	Page
Layer 2 Priority Commands			
switchport priority default	Sets a port priority for incoming untagged frames	IC	4-165
queue bandwidth	Assigns round-robin weights to the priority queues	GC	4-166
queue cos map	Assigns class of service values to the priority queues	IC	4-167
show queue bandwidth	Shows round-robin weights assigned to the priority queues	PE	4-168
show queue cos-map	Shows the class of service map	PE	4-168
show interfaces switchport	Displays the administrative and operational status of an interface	PE	4-119
Layer 3 and 4 Priority Commands			
map ip precedence	Enables IP precedence class of service mapping	GC	4-169
map ip precedence	Maps IP precedence value to a class of service	IC	4-169
map ip dscp	Enables IP DSCP class of service mapping	GC	4-170
map ip dscp	Maps IP DSCP value to a class of service	IC	4-171
map ip port	Enables TCP/UDP class of service mapping	GC	4-172
map ip port	Maps TCP/UDP socket to a class of service	IC	4-172
show map ip precedence	Shows the IP precedence map	PE	4-173
show map ip dscp	Shows the IP DSCP map	PE	4-173
show map ip port	Shows the IP port map	PE	4-174

Layer 2 Priority Commands

switchport priority default

Use this command to set a priority for incoming untagged frames, or the priority of frames received by the device connected to the specified interface. Use the **no** form to restore the default value.

Syntax

switchport priority default *default-priority-id*
no switchport priority default

default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero.

Command Mode

Interface Configuration (Ethernet, Port Channel)

© 2004 Foundry Networks, Inc.

Command Usage

- The precedence for priority mapping is IP Precedence or IP DSCP, and default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- This switch provides four priority queues for each port. It is configured to use Weighted Round Robin, which can be viewed with the **queue bandwidth** command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 0 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
```

queue bandwidth

Use this command to assign Weighted Round-Robin (WRR) weights to the four class of service (CoS) priority queues. Use the **no** form to restore the default weights.

Syntax

queue bandwidth *weightX...weightY*
no queue bandwidth

weightX...weightY - The ratio of weights for queues used by the WRR scheduler. (See below).

Default Setting

EdgeIron 24G-A, 48G								
Priority	1	2	4	6	8	10	12	14
Queue	0	1	2	3	4	5	6	7

EdgeIron 4802CF, 2402CF				
Priority	1	4	16	64
Queue	0	1	2	3

EdgeIron 24G				
Priority	16	64	128	240
Queue	0	1	2	3

Command Mode

Global Configuration

Command Usage

WRR allows bandwidth sharing at the egress port by defining scheduling weights.

 © 2004 Foundry Networks, Inc.

Example

The following example shows how to assign WRR weights of 1, 3, 5 and 7 to the CoS priority queues 0, 1, 2 and 3:

```
Console(config)#queue bandwidth 1 3 5 7
Console(config)#
```

Related Commands

show queue bandwith (4-168)

queue cos-map

Use this command to assign class of service (CoS) values to the priority queues (i.e., hardware output queues EdgeIron 4802CF, 2402CF and 24G: 0-3, and EdgeIron 24G-A and 48G: 0-7). Use the **no** form set the CoS map to the default values.

Syntax

queue cos-map *queue_id* [*cos1 ... cosn*]
no queue cos-map

- *queue_id* - The queue ID of the CoS priority queue.
- Ranges are 0 to 3, where 3 is the highest CoS priority queue.
- *cos1 .. cosn* - The CoS values that are mapped to the queue ID. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

Default Setting

This switch supports Class of Service by using four priority queues, with Weighted Round Robin for each port. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

	Queue			
	1	**2**	**3**	**4**
Priority		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

Note: CoS priority mappings are configured per-port. However, due to a hardware limitations all mappings are applied system-wide. In other words, no matter which port is set for CoS mapping, it's applies globally to all ports.

Command Mode

Interface Configuration (Ethernet, Port Channel)

© 2004 Foundry Networks, Inc.

Command Usage

CoS assigned at the ingress port is used to select a CoS priority at the egress port.

Example

The following example shows how to map CoS values 0, 1 and 2 to CoS priority queue 0, value 3 to CoS priority queue 1, values 4 and 5 to CoS priority queue 2, and values 6 and 7 to CoS priority queue 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0 1 2
Console(config-if)#queue cos-map 1 3
Console(config-if)#queue cos-map 2 4 5
Console(config-if)#queue cos-map 3 6 7
Console(config-if)#
```

Related Commands

show queue cos-map (4-168)

show queue bandwidth

Use this command to display the Weighted Round-Robin (WRR) bandwidth allocation for the four class of service (CoS) priority queues.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue bandwidth
 Queue ID Weight
 -------- ------
        0      1
        1      4
        2     16
        3     64
Console#
```

show queue cos-map

Use this command to show the class of service priority map.

Syntax

show queue cos-map [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

 © 2004 Foundry Networks, Inc.

Command Mode

Privileged Exec

Example

```
Console#sh queue cos-map ethernet 1/11
Information of Eth 1/11
 CoS Value     : 0 1 2 3 4 5 6 7
 Priority Queue: 2 0 1 3 4 5 6 7
Console#
```

Layer 3 and 4 Priority Commands

map ip precedence (Global Configuration)

Use this command to enable IP precedence mapping (i.e., IP Type of Service). Use the **no** form to disable IP precedence mapping.

Syntax

map ip precedence
no map ip precedence

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP precedence mapping globally:

```
Console(config)#map ip precedence
Console(config)#
```

map ip precedence (Interface Configuration)

Use this command to set IP precedence priority (i.e., IP Type of Service priority). Use the **no** form to restore the default table.

Syntax

map ip precedence *ip-precedence-value* **cos** *cos-value*
no map ip precedence

- *precedence-value* - 3-bit precedence value. (Range: 0-7)
- *cos-value* - Class-of-Service value (Range: 0-7)

 © 2004 Foundry Networks, Inc.

Default Setting

The list below shows the default priority mapping.

IP Precedence Value	CoS Value
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence values are mapped to default Class of Service values on a one-to-one basis according to recommendations in the IEEE 802.1p standard, and then mapped to the queue defaults.
- This command sets the IP Precedence for all interfaces.

Example

The following example shows how to map IP precedence value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

map ip dscp (Global Configuration)

Use this command to enable IP DSCP mapping (i.e., Differentiated Services Code Point mapping). Use the **no** form to disable IP DSCP mapping.

Syntax

map ip dscp
no map ip dscp

Default Setting

Disabled

Command Mode

Global Configuration

 © 2004 Foundry Networks, Inc.

Command Usage

- The precedence for priority mapping is IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP DSCP mapping globally:

```
Console(config)#map ip dscp
Console(config)#
```

map ip dscp (Interface Configuration)

Use this command to set IP DSCP priority (i.e., Differentiated Services Code Point priority). Use the **no** form to restore the default table.

Syntax

map ip dscp *dscp-value* **cos** *cos-value*
no map ip dscp

- *dscp-value* - 8-bit DSCP value. (Range: 0-255)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The list below shows the default priority mapping. Note that all the DSCP values that are not specified are mapped to CoS value 0.

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then mapped to the queue defaults.
- This command sets the DSCP Priority for all interfaces.

 © 2004 Foundry Networks, Inc.

Example

The following example shows how to map IP DSCP value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

map ip port (Global Configuration)

Use this command to enable IP port mapping (i.e., class of service mapping for TCP/UDP sockets). Use the **no** form to disable IP port mapping.

Syntax

map ip port
no map ip port

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

Example

The following example shows how to enable TCP/UDP port mapping globally:

```
Console(config)#map ip port
Console(config)#
```

map ip port (Interface Configuration)

Use this command to set IP port priority (i.e., TCP/UDP port priority). Use the **no** form to remove a specific setting.

Syntax

map ip port *port-number* **cos** *cos-value*
no map ip port *port-number*

- *port-number* - 16-bit TCP port number. (Range: 0-65535)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- This command sets the IP port priority for all interfaces.

 © 2004 Foundry Networks, Inc.

Example

The following example shows how to map HTTP traffic to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0
Console(config-if)#
```

show map ip precedence

Use this command to show the IP precedence priority map.

Syntax

show map ip precedence [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 5          0   0
  Eth 1/ 5          1   1
  Eth 1/ 5          2   2
  Eth 1/ 5          3   3
  Eth 1/ 5          4   4
  Eth 1/ 5          5   5
  Eth 1/ 5          6   6
  Eth 1/ 5          7   7
Console#
```

Related Commands

map ip precedence (Global Configuration) (4-169)
map ip precedence (Interface Configuration) (4-169)

show map ip dscp

Use this command to show the IP DSCP priority map.

Syntax

show map ip dscp [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

© 2004 Foundry Networks, Inc.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
.
.
.
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

Related Commands

map ip dscp (Global Configuration) (4-170)
map ip dscp (Interface Configuration) (4-171)

show map ip port

Use this command to show the IP port priority map.

Syntax

show map ip port [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

The following shows that HTTP traffic has been mapped to CoS value 0:

```
Console#show map ip port
TCP port mapping status: disabled

 Port      Port no. COS
 --------- -------- ---
  Eth 1/ 5       80   0
Console#
```

Related Commands

map ip port (Global Configuration) (4-172)
map ip port (Interface Configuration) (4-172)

 © 2004 Foundry Networks, Inc.

Mirror Port Commands

This section describes how to configure port mirror sessions.

Command	Function	Mode	Page
port monitor	Configures a mirror session	IC	4-175
show port monitor	Shows the configuration for a mirror port	PE	4-176

port monitor

Use this command to configure a mirror session. Use the **no** form to clear a mirror session.

Syntax

port monitor *interface* [**rx** | **tx** | **both**]
no port monitor *interface*

- *interface*
  - **ethernet** *unit*/*port* (source port)
    - *unit* - Switch (unit 1).
    - *port* - Port number.
- **rx** - Mirror received packets.
- **tx** - Mirror transmitted packets.
- **both** - Mirror both received and transmitted packets.

Default Setting

No mirror session is defined. When enabled, the default mirroring is for both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet, destination port)

Command Usage

- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- The destination port is set by specifying an Ethernet interface.
- The source and destination port speeds should match, otherwise traffic may be dropped from the source port.
- EdgeIron 4802CF, 2402CF:
  - You can create more than one mirror session, but all must share the same destination port. However, you should avoid sending too much traffic to the destination port from multiple source ports.

Note: The 4802CF may only set one mirror-to port, but you can set as many as 49 mirror-from ports.

© 2004 Foundry Networks, Inc.

- EdgeIron 24G-A, 24G, 48G:
  - You can create only one mirror port session.
  - The source and destination ports have to be either both in the port range 1-12 or both in the port range 13-24; or in the case of the 48G port range 25-36 or port range 37-48 as well.

Example

The following example configures the switch to mirror all packets from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

Related Commands

show port monitor (4-176)

show port monitor

Use this command to display mirror information.

Syntax

show port monitor [*interface*]

interface

- **ethernet** *unit*/*port* (source port)
  - *unit* - Switch (unit 1).
  - *port* - Port number.

Default Setting

Shows all sessions.

Command Mode

Privileged Exec

Command Usage

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example

The following shows mirroring configured from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination port(listen port):Eth1/1
 Source port(monitored port)  :Eth1/6
 Mode                         :RX/TX
Console#
```

Related Commands

port monitor (4-175)

 © 2004 Foundry Networks, Inc.

Port Trunking Commands

Ports can be statically grouped into an aggregate link to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP), also known as 802.1ad, to automatically negotiate a trunk link between this switch and another network device. For dynamic trunks, the switches have to comply with LACP. This switch supports up to six trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

To determine the load spread over the ports in a trunk there are three algorithms that may be used in combination with a hashing algorithm. The load balance algorithm can be based on either MAC SA, MAC DA, IP SA, IP DA, VID or protocol type (see reg 0x24 from Broadcom 5632 data sheet). Based on the selected key(s), the chip itself will use a (proprietary) CRC-like circuit to generate a value. Then, obtain the remainder of this value and the number of ports in that trunk to decide the port.

Command	Function	Mode	Page
Manual Configuration Commands			
interface port-channel	Configures a trunk and enters interface configuration mode for the trunk	GC	4-109
channel-group	Adds a port to a trunk	IC	4-178
Dynamic Configuration Command			
lacp	Configures LACP for the current interface	IC	4-178
lacp system-priority	Configures a port's LACP system priority	IC (Ethernet)	4-179
lacp admin-key	Configures a port's administration key	IC (Ethernet)	4-180
lacp admin-key	Configures an port channel's administration key	IC (Port Channel)	4-181
lacp port-priority	Configures a port's LACP port priority	IC (Ethernet)	4-181
Trunk Status Display Command			
show interfaces status port-channel	Shows trunk information	NE, PE	4-117
show lacp	Shows LACP information	PE	4-182

Guidelines for Creating Trunks

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- The maximum number of ports that can be combined as a static trunk:
  - EdgeIron 4802CF, 2402CF: Four 10/100 Mbps ports, and two 1000 Mbps ports.
  - EdgeIron 24G-A, 24G, 48G: Six 1000 Mbps ports.
- The ports at both ends of a connection must be configured as trunk ports.
- All ports in a trunk must consist of the same media type (i.e., twisted-pair or fiber).
- All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.

© 2004 Foundry Networks, Inc.

- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

channel-group

Use this command to add a port to a trunk. Use the **no** form to remove a port from a trunk.

Syntax

channel-group *channel-id*
no channel-group

channel-id - Trunk index (Range: 1-6)

Default Setting

A new trunk contains no ports.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Static trunks have to be manually configured at both ends of the link.
- Use **no channel-group** to remove a port group from a trunk.
- Use **no interfaces port-channel** to remove a trunk from the switch.
- All links in a trunk must operate at the same data rate and duplex mode.

Example

The following example creates trunk 1 and then adds port 11:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

Dynamic Trunk Configuration Commands

lacp

Use this command to enable 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

Syntax

lacp
no lacp

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

 © 2004 Foundry Networks, Inc.

Command Usage

- The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- If more than four ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Example

The following shows LACP enabled on ports 11-13. Because LACP has also been enabled on the ports at the other end of the links, the **show interfaces status port-channel 1** command shows that Trunk 1 has been established.

```
Console(config)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic information:
  Port type: 100TX
  Mac address: 00-30-F1-47-58-4E
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Flow control: Disabled
  Port security: Disabled
  Port security action: None
 Current status:
  Created by: Lacp
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 100full
  Flow control type: None
  Member Ports: Eth1/11, Eth1/12, Eth1/13,
Console#
```

lacp system-priority

This command configures a port's LACP system priority. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **system-priority** *priority*
no lacp {**actor** | **partner**} **system-priority**

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *priority* - This priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

Default Setting

32768

 © 2004 Foundry Networks, Inc.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Port must be configured with the same system priority to join the same LAG.
- System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

lacp admin-key (Ethernet Interface)

This command configures a port's LACP administration key. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **admin-key** *key*
[**no**] **lacp** {**actor** | **partner**} **admin-key**

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *key* - The port admin key must be set to the same value for ports that belong to the same link aggregation group (LAG). (Range: 0-65535)

Default Setting

0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel admin key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

 © 2004 Foundry Networks, Inc.

lacp admin-key (Port Channel)

This command configures a port channel's LACP administration key string. Use the **no** form to restore the default setting.

Syntax

lacp admin-key *key*
[**no**] **lacp admin-key**

- *key* - The port channel admin key is used to identify a specific link aggregation group (LAG) during local LACP setup on this switch. (Range: 0-65535)

Default Setting

0

Command Mode

Interface Configuration (Port Channel)

Command Usage

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group. Note that when the LAG is no longer used, the port channel admin key is reset to 0.

Example

```
Console(config)#interface port channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

lacp port-priority

This command configures LACP port priority. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **port-priority** *priority*
no lacp {**actor** | **partner**} **port-priority**

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *priority* - LACP port priority is used to select a backup link. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Setting a lower value indicates a higher effective priority.
- If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.

© 2004 Foundry Networks, Inc.

- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

show lacp

This command displays LACP information.

Syntax

show lacp [*port-channel*] {**counters** | **internal** | **neighbors** | **sys-id**}

- *port-channel* - Local identifier for a link aggregation group. (Range: 1-6)
- **counters** - Statistics for LACP protocol messages.
- **internal** - Configuration settings and operational state for local side.
- neighbors - Configuration settings and operational state for remote side.
- **sys-id** - Summary of system priority and MAC address for all channel groups.

Default Setting

Port Channel: all

Command Mode

Privileged Exec

Example

```
Console#show lacp 1 counters
Channel group : 1 ------------------------------------------------------------
Eth 1/ 1 --------------------------------------------------------------------
  LACPDUs Sent : 21
  LACPDUs Received : 21
  Marker Sent : 0
  Marker Received : 0
  LACPDUs Unknown Pkts : 0
  LACPDUs Illegal Pkts : 0
.
.
.
```


© 2004 Foundry Networks, Inc.

Parameter	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
LACPDUs Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
LACPDUs Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

```
Console#show lacp 1 internal
Channel group : 1
------------------------------------------------------------------------------
Oper Key : 4
Admin Key : 0
Eth 1/1
------------------------------------------------------------------------------
  LACPDUs Internal : 30 sec
  LACP System Priority : 32768
  LACP Port Priority : 32768
  Admin Key : 4
  Oper Key : 4
  Admin State : defaulted, aggregation, long timeout, LACP-activity
  Oper State : distributing, collecting, synchronization,
               aggregation, long timeout, LACP-activity
```

 © 2004 Foundry Networks, Inc.

Parameter	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: Expired – The actor's receive machine is in the expired state; Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

```
Console#show lacp 1 neighbors
Channel group 1 neighbors
------------------------------------------------------------------------
Eth 1/1
------------------------------------------------------------------------
  Partner Admin System ID : 32768, 00-00-00-00-00-00
  Partner Oper System ID : 32768, 00-00-00-00-00-01
  Partner Admin Port Number : 1
  Partner Oper Port Number : 1
  Port Admin Priority : 32768
  Port Oper Priority : 32768
  Admin Key : 0
  Oper Key : 4
  Admin State : defaulted, distributing, collecting, synchronization,
                long timeout,
  Oper State : distributing, collecting, synchronization, aggregation,
               long timeout, LACP-activity
.
.
.
```

Parameter	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

```
Console#show lacp sysid
Channel group    System Priority    System MAC Address
-----------------------------------------------------------------
            1              32768     00-30-F1-8F-2C-A7
            2              32768     00-30-F1-8F-2C-A7
            3              32768     00-30-F1-8F-2C-A7
            4              32768     00-30-F1-8F-2C-A7
            5              32768     00-30-F1-8F-2C-A7
            6              32768     00-30-F1-8F-2C-A7
Console#
```

Parameter	Description
Channel group	A link aggregation group configured on this switch.
System Priority*	LACP system priority for this channel group.
System MAC Address*	System MAC address.

* The LACP system priority and system MAC address are concatenated to form the LAG system ID.

© 2004 Foundry Networks, Inc.

Rate Limiting Commands

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Command	Function	Mode	Page
rate-limit	Configures the maximum input or output rate for an interface	IC	4-186

rate-limit

Use this command to define and enable a rate limit for a specific interface. Use this command without specifying a rate to restore the default rate. Use the **no** form to disable rate limiting.

Syntax

rate-limit {**input** | **output**} [*rate*]
no rate-limit {**input** | **output**}

- **input** – Input rate
- **output** – Output rate
- *rate* – Maximum value in Mbps.

Default Setting

Fast Ethernet interface – 100 Mbps
Gigabit Ethernet interface – 1000 Mbps

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The range is:
  - Fast Ethernet interface – 1 to 100 Mbps
  - Gigabit Ethernet interface – 8 to 1000 Mbps
- Resolution – The increment of change:
  - Fast Ethernet interface – 1 Mbps
  - Gigabit Ethernet interface – 8 Mbps

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 8
Console(config-if)#
```

 © 2004 Foundry Networks, Inc.

Appendix A
Using Syslog

Overview

This appendix describes how to display Syslog messages and how to configure the Syslog facility, and lists the Syslog messages that a Foundry EdgeIron switch can display during standard operation.

A Foundry device's software can write syslog messages to provide information at the following severity levels:

- Emergencies
- Alerts
- Critical
- Errors
- Warnings
- Notifications
- Informational
- Debugging

The device writes the messages to a local buffer.

You also can specify the IP address or host name of up to five Syslog servers. When you specify a Syslog server, the Foundry device writes the messages both to the system log and to the Syslog server.

Using a Syslog server ensures that the messages remain available even after a system reload. The Foundry device's local Syslog buffer is cleared during a system reload or reboot, but the Syslog messages sent to the Syslog server remain on the server.

The Syslog service on a Syslog server receives logging messages from applications on the local host or from devices such as a Layer 2 Switch or Layer 3 Switch. Syslog adds a time stamp to each received message and directs messages to a log file. Most Unix workstations come with Syslog configured. Some third-party vendor products also provide Syslog for Windows.

Syslog uses UDP port 514 and each Syslog message thus is sent with destination port 514. Each Syslog message is one line with Syslog message format. The message is embedded in the text portion of the Syslog format. There are several subfields in the format. Keywords are used to identify each subfield, and commas are delimiters. The subfield order is insensitive except that the text subfield should be the last field in the message. All the subfields are optional.

© 2004 Foundry Networks, Inc.

Displaying Syslog Messages

To display the Syslog messages in the device's local buffer, enter the following command at the Privileged Exec level of the CLI:

```
Console#sh logging ram
Syslog logging: Enable
History logging in RAM: level debugging
[3] 0:1:32 1/1/1
   "VLAN 1 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[2] 0:1:32 1/1/1
   "STP topology change notification."
   level: 6, module: 6, function: 1, and event no.: 1
[1] 0:1:32 1/1/1
   "Unit 1, Port 23 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[0] 0:1:32 1/1/1
   "System coldStart notification."
   level: 6, module: 6, function: 1, and event no.: 1
Console#
```

For information about the Syslog configuration information, time stamps, and dynamic and static buffers, see "System Logs" on page 3-16.

Configuring the Syslog Service

The procedures in this section describe how to perform the following Syslog configuration tasks:

- Specify a Syslog server. You can configure the Foundry device to use up to five Syslog servers. (Use of a Syslog server is optional. The system can hold up to up to 2048 Syslog messages in RAM memory and up to 4096 messages in Flash memory.)
- Change the level of messages the system logs.
- Display the Syslog configuration.
- Clear the local Syslog buffer.

Syslog logging is disabled by default, with the following settings:

- Messages of all severity levels (Emergencies through Debugging) are logged.
- No Syslog server is specified.

Displaying the Syslog Configuration

To display the Syslog parameters currently in effect on a Foundry EdgeIron device, enter the following command from the Privileged Exec level of the CLI:

```
Console#show logging trap
Syslog logging: Enable
REMOTELOG status: disable
REMOTELOG facility type: local use 7
REMOTELOG level type: Debugging messages
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
```


© 2004 Foundry Networks, Inc.

Syntax: show logging {flash | ram | trap}

The Syslog display shows the following configuration information.

Table A.1: CLI Display of Syslog Configuration

This Field...	Displays...
Syslog logging	The state (enabled or disabled) of logging on the switch.
REMOTELOG Status	The state (enabled or disabled) of logging to a remote Syslog server.
REMOTELOG Facility Type	A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service.
REMOTELOG Level Type	One of the Syslog levels from 0 (Emergencies) to 7 (Debugging). Messages sent include the selected level up through level 0.
REMOTELOG Server IP Address	Up to five IP addresses of Syslog servers.

Flash and RAM Buffers

The software provides two separate buffers:

- Flash - Permanently stored in the switch.
- RAM - Memory flushed on power reset.

Error messages that are logged to flash memory remain stored in the switch even after a power reset. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded.

The switch can store up to 2048 log entries in temporary random access memory (RAM; i.e., memory flushed on power reset). The switch periodically copies log messages in RAM to flash memory, depending on the error level limit configured. The flash error level limit must be equal to or less than the RAM level limit.

The flash and RAM buffers are both displayed using the following commands:

```
Console#sh logging ram
Syslog logging: Enable
History logging in RAM: level debugging
[3] 0:1:32 1/1/1
   "VLAN 1 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[2] 0:1:32 1/1/1
   "STP topology change notification."
   level: 6, module: 6, function: 1, and event no.: 1
[1] 0:1:32 1/1/1
   "Unit 1, Port 23 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[0] 0:1:32 1/1/1
   "System coldStart notification."
   level: 6, module: 6, function: 1, and event no.: 1
Console#
```


© 2004 Foundry Networks, Inc.

```
Console#sh logging flash
Syslog logging: Enable
History logging in FLASH: level errors
[9] 13:30:42 2/28/4
   "VLAN 1 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[8] 13:30:42 2/28/4
   "STP topology change notification."
   level: 6, module: 6, function: 1, and event no.: 1
[7] 13:30:12 2/28/4
   "Unit 1, Port  8 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[6] 13:30:8 2/28/4
   "Unit 1, Port  8 link-down notification."
   level: 6, module: 6, function: 1, and event no.: 1
[5] 13:30:8 2/28/4
   "VLAN 1 link-down notification."
   level: 6, module: 6, function: 1, and event no.: 1
[4] 13:20:6 3/3/4
   "VLAN 1 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[3] 13:20:6 3/3/4
   "STP topology change notification."
   level: 6, module: 6, function: 1, and event no.: 1
[2] 13:19:36 3/3/4
   "Unit 1, Port  8 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[1] 13:19:31 3/3/4
   "Unit 1, Port  6 link-down notification."
   level: 6, module: 6, function: 1, and event no.: 1
[0] 13:19:31 3/3/4
   "VLAN 1 link-down notification."
   level: 6, module: 6, function: 1, and event no.: 1
Console#
```

When you clear log entries, you can selectively clear the flash or RAM, or you can clear both. For example, to clear only the RAM, enter the following command at the Privileged Exec level:

```
EdgeIron# clear logging ram
```

Syntax: clear logging [ram | flash]

You can specify **ram** to clear the RAM buffer or **flash** to clear the flash buffer. If you do not specify a buffer, both buffers are cleared.

Time Stamps

The contents of the time stamp depends on whether the system time and date has been set manually or by SNTP.

- If the system clock has been set, the date and time are shown in the following format:
  - hh:mm:ss m/d/y

    where:
    - hh – hours
    - mm – minutes
    - ss – seconds
    - m – month
    - d – day
    - y – year

  For example, “22:34:15 2/28/4" means February 28, 2004 at 10:34 PM and 15 seconds.
- If the system clock is not set, the time stamp shows the time and date since the device was booted, starting from 00:00:00 1/1/1.

© 2004 Foundry Networks, Inc.

Example of Syslog Messages on a Device Whose Onboard Clock Is Set

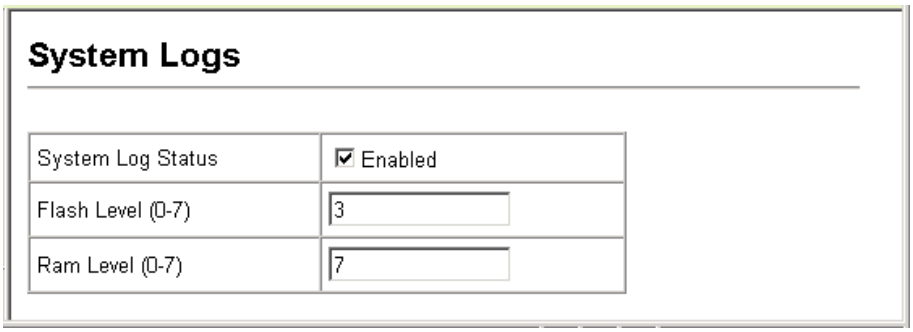
The example shows the format of messages on a device whose onboard system clock has been set. Each time stamp shows the month, the day, and the time of the system clock when the message was generated. For example, the system time when the most recent message (the one at the top) was generated was February 28, 2004 at 1:30 PM and 12 seconds.

```
Console#show logging ram
Syslog logging: Enable
History logging in RAM: level debugging
[11] 13:30:12 2/28/4
   "Unit 1, Port  8 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[10] 13:30:8 2/28/4
   "Unit 1, Port  8 link-down notification."
   level: 6, module: 6, function: 1, and event no.: 1
[9] 13:30:8 2/28/4
   "VLAN 1 link-down notification."
   level: 6, module: 6, function: 1, and event no.: 1
```

Displaying and Configuring Syslog Buffer Parameters Using the Web Management Interface

To configure Syslog parameters using the Web management interface, use the following procedure:

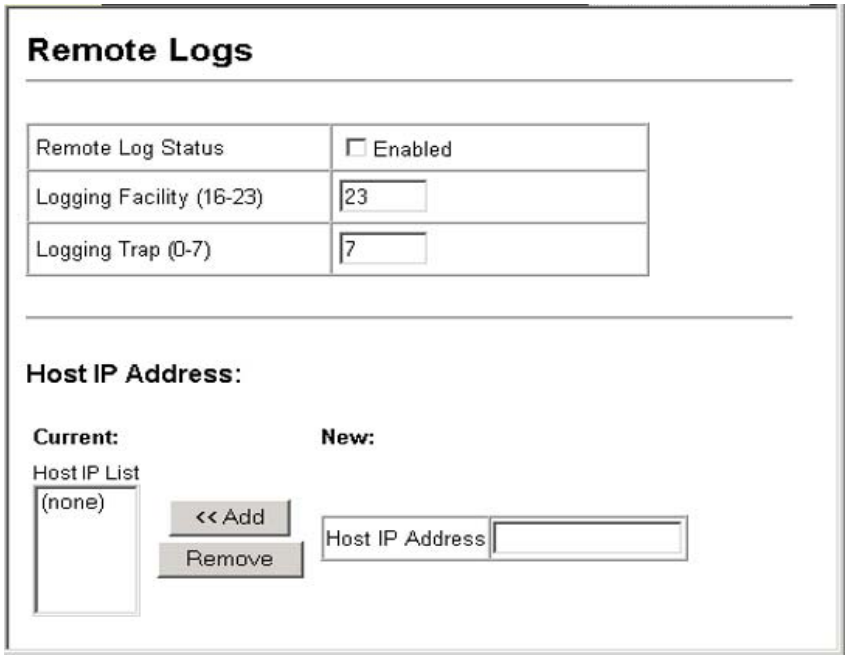
1. Log on to the device using a valid user name and password for read-write access. The System Information page is displayed.
2. Select Log from the System menu.
3. Select the System Logs link to display the following page:



4. Check or clear the check box next to System Log Status to enable or disable the Syslog service on the device. The service is enabled by default.
5. Select the maximum message level you want the device to log to RAM and flash. All the levels are logged to RAM by default.
6. Click Apply to save the changes to the device's running-config file.

© 2004 Foundry Networks, Inc.

7. To enable logging to Syslog servers and view a list of the servers that have been defined, click the Remote Logs link.



8. Check or clear the check box next to Remote Log Status to enable or disable logging to Syslog servers. The remote logging service is disabled by default.
9. Select the maximum message level you want the device to log to Syslog servers. All the levels are logged by default.

Disabling or Re-Enabling Syslog

Syslog is enabled by default. To disable or re-enable it, use one of the following methods.

USING THE CLI

To disable it, enter the following command at the global CONFIG level:

```
EdgeIron(config)# no logging on
```

Syntax: [no] logging on

To re-enable logging, enter the following command:

```
EdgeIron(config)# logging on
```

This command enables local Syslog logging with the following defaults:

- Messages of all severity levels (Emergencies through Debugging) are logged.
- No Syslog server is specified.

Specifying a Syslog Server

To specify a Syslog server, enter the following command:

USING THE CLI

```
EdgeIron(config)# logging host 10.0.0.99
```

Syntax: [no] logging host <ip-address>

© 2004 Foundry Networks, Inc.

Using The Web Management Interface

See the section "Remote Logs Configuration" on page 3-17.

Specifying an Additional Syslog Server

USING THE CLI

To specify an additional Syslog server, enter the **logging host** <ip-addr> command again, as in the following example. You can specify up to five Syslog servers.

```
EdgeIron(config)# logging host 10.0.0.99
```

Syntax: [no] logging host <*ip-address*>

Changing the Log Facility

The Syslog daemon on the Syslog server uses a facility to determine where to log the messages from the Foundry device. The default facility for messages the Foundry EdgeIron device sends to the Syslog server is "local use 7." You can change the facility using the following command.

NOTE: You can specify only one facility. If you configure the Foundry device to use two Syslog servers, the device uses the same facility on both servers.

```
EdgeIron(config)# logging facility 16
```

Syntax: [no] logging facility <type>

The <type> can be one of the following facility numbers:

- 16 – local use 0
- 17 – local use 1
- 18 – local use 2
- 19 – local use 3
- 20 – local use 4
- 21 – local use 5
- 22 – local use 6
- 23 – local use 7

USING THE WEB MANAGEMENT INTERFACE

See the section "Remote Logs Configuration" on page 3-17.

Clearing the Syslog Messages from the Local Buffer

To clear the Syslog messages stored in the Foundry device's local buffer, use the following CLI command:

```
EdgeIron# clear logging
```

Syntax: clear logging [flash | ram]

 © 2004 Foundry Networks, Inc.

Syslog Messages

Table A.2 lists all of the Syslog messages. The messages are listed by message level, in the following order:

- Emergencies (none)
- Alerts
- Critical (none)
- Errors
- Warnings
- Notifications
- Informational
- Debugging

NOTE: In the messages displayed %s is substitute with a string, and %1d is replaced with integer values.

Table A.2: Foundry Syslog Messages

Message Level	Message	Explanation
Critical	%s create task fail	The created task has failed.
Error	%s switch to default	The switch has encountered an abnormal case.
Critical	Allocate %s memory fail	Comand to allocate memory has failed.
Critical	Free %s memory fail	Command to free memory has failed.
Informative	Unit %1d, fan %1d fail	A fan has failed.
Error	%s funtion fails	A software function has failed.
Informative	System coldStart notification	A coldstart has occured.
Informative	System warmStart notification	A warmstart has occured.
Informative	Unit %1d, Port %1d link-up notification	A link to a port has been established.
Informative	Unit %1d, Port %1d link-down notification	A link to a port has failed.
Informative	Trunk %1d link-up notification	A link to a trunk has been established.
Informative	Trunk %1d link-down notification	A link to a trunk has failed.
Informative	VLAN %1d link-up notification	A link to a VLAN has been established.
Informative	VLAN %1d link-down notification	A link to a VLAN has failed.
Informative	Authentication failure notification	The user authentication procedure has failed.

© 2004 Foundry Networks, Inc.

Table A.2: Foundry Syslog Messages (Continued)

Message Level	Message	Explanation
Informative	STA root change notification	The root of the spanning tree has changed.
Informative	STA topology change notification	The spanning tree topology has changed.
Informative	RMON rising alarm	A RMON warning has occured and is increasing in severity.
Informative	RMON falling alarm notification	A RMON warning has occured and is decreasing in severity.
Informative	Unit %1d, %s power change to %s	The power status of the device unit has changed.
Informative	Loopback test failure	The loopback test has failed.
Informative	Fan Recover, unit=[%d], fanIndex=[%1d]	A fan has recovered from a failure condition.
Informative	Ipfilter reject, mode=[%1d.%1d.%1d.%1d]	The IP filter has rejected some data packets.
Warning	DHCP request failed - will retry later	A DHCP request has failed and will attempt resending the request later.
Warning	DHCP server responded	A response from a DHCP server has been received.
Informative	SMTP connect host %s failure	The switch has failed to connect ot the SMTP host.
Informative	MainBoardVerMismatch:%s	There is a mismatch in the firmware version specified.
Informative	ModuleVerMismatch:%s	The firmware version of the module mismatches the device version.
Informative	ModuleInsertion:%s	An optional module was inserted in to the device.
Informative	ModuleRemoval:%s	A module was removed from the device.

© 2004 Foundry Networks, Inc.

© 2004 Foundry Networks, Inc.

Appendix B
Troubleshooting

Troubleshooting Chart

Troubleshooting Chart	
Symptom	**Action**
Cannot connect using Telnet, Web browser, or SNMP software	• Be sure to have configured the agent with a valid IP address, subnet mask and default gateway. • Be sure that your management station has management VLAN access to the switch (default is VLAN 1). • Check that you have a valid network connection to the switch and that the port you are using has not been disabled. • Check network cabling between the management station and the switch. • If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet sessions permitted. Try connecting again at a later time.
Cannot access the on-board configuration program via a serial port connection	• Be sure to have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity and 9600 bps. • Check that the null-modem serial cable conforms to the pin-out connections provided in Appendix B.
Forgot or lost the password (Applicable to EdgeIron 2402CF, 4802CF and 24G only.)	• Set the switch to its default configuration. Make a direct connection to the switch's console port and power cycle the switch. Immediately after powering on, press <Ctrl><u> to access the system file menu.]Select <D> to delete all user-defined configuration files. Press <Q> to boot the switch.

© 2004 Foundry Networks, Inc.

© 2004 Foundry Networks, Inc.

Appendix C
Upgrading Firmware via the Serial Port

Note: The following procedure is only applicable to the EdgeIron 2402CF, 4802CF and 24G.

The switch contains three firmware components that can be upgraded; the diagnostics (or Boot-ROM) code, runtime operation code, and the loader code. The runtime code can be upgraded via the switch's RS-232 serial console port, via a network connection to a TFTP server, or using SNMP management software. The diagnostics and loader code can be upgraded only via the switch's RS-232 serial console port.

Note: You can use the switch's web interface to download runtime code via TFTP. Downloading large runtime code files via TFTP is normally much faster than downloading via the switch's serial port.

You can upgrade switch firmware by connecting a PC directly to the serial Console port on the switch's front panel and using VT100 terminal emulation software that supports the XModem protocol. (See "Required Connections" on page 2-2.)

1. Connect a PC to the switch's Console port using a null-modem or crossover RS-232 cable with a female DB-9 connector.
2. Configure the terminal emulation software's communication parameters to 9600 baud, 8 data bits, 1 stop bit, no parity, and set flow control to *none*.
3. Power cycle the switch.
4. When the switch initialization screen appears, enter firmware-download mode by pressing <Ctrl><u> immediately after power on. Screen text similar to that shown below displays:

```
File Name                        S/Up Type Size       Create Time
-------------------------------- ---- ---- ---------- -----------
$certificate                       0    7      20480  00:38:34
$logfile_1                         0    3         64  00:00:02
Factory_Default_Config.cfg         0    5       2574  00:00:12
diag_1000                          1    1     116228  00:00:00
r_20019                            1    2    1536972  00:00:01
set-ip.cfg                         1    5       2690  00:40:44
-------------------------------- ---- ---- ---------- ----------
[X]modem Download  [D]elete File  [S]et Startup File
[C]hange Baudrate  [Q]uit
Select>
```

 © 2004 Foundry Networks, Inc.

5. Press <C> to change the baud rate of the switch's serial connection.
6. Press <B> to select the option for 115200 baud.

   There are two baud rate settings available, 9600 and 115200. Using the higher baud rate minimizes the time required to download firmware code files.
7. Set your PC's terminal emulation software to match the 115200 baud rate. Press <Enter> to reset communications with the switch.

```
Select>
Change baudrate [A]9600 [B]115200
Baudrate set to 115200
```

8. Check that the switch has sufficient flash memory space for the new code file before starting the download.

   You can store a maximum of only two runtime and two diagnostic code files in the switch's flash memory. Use the **[D]elete File** command to remove a runtime or diagnostic file.
9. Press <X> to start to download the new code file.

   If using Windows HyperTerminal, click the "Transfer" button, and then click "Send File...." Select the XModem Protocol and then use the "Browse" button to select the required firmware code file from your PC system. The "Xmodem file send" window displays the progress of the download procedure.

Note: The download file must be a vaild binary software file from Foundry for the target switch.

10. After the file has been downloaded, you are prompted with "Update Image File:" to specify the type of code file. Press <R> for runtime code, <D> for diagnostic code, or ,<L> for loader code.

Caution: If you select <L> for loader code, be sure the file is a valid loader code file for the switch. If you download an invalid file, the switch will not be able to boot. Unless absolutely necessary, do not attempt to download loader code files.

11. Specify a name for the downloaded code file. File names are case-sensitive, should be from 1 to 31 characters, not contain slashes (\ or /), and the leading letter of the file name should not be a period (.). (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

© 2004 Foundry Networks, Inc.

For example, the following screen text shows the download procedure for a runtime code file:

```
Select>
Xmodem Receiving Start ::
Image downloaded to buffer.


        [R]untime
        [D]iagnostic
        [L]oader (Warning: you sure what you are doing?)
Update Image File:r
Diagnostic Image Filename : r_20019
Updating file system.
File system updated.
[Press any key to continue]
```

12. To set the new downloaded file as the startup file, use the **[S]et Startup File** menu option.
13. When you have finished downloading code files, use the **[C]hange Baudrate** menu option to change the baud rate of the switch's serial connection back to 9600 baud.
14. Set your PC's terminal emulation software baud rate back to 9600 baud. Press <Enter> to reset communications with the switch.
15. Press <Q> to quit the firmware-download mode and boot the switch.

 © 2004 Foundry Networks, Inc.

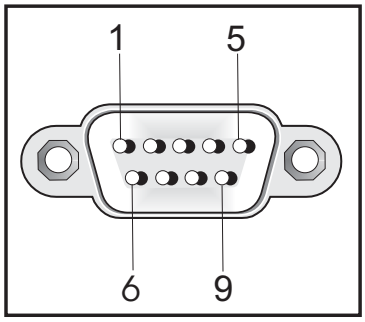
© 2004 Foundry Networks, Inc.

Appendix D
Pin Assignments

Console Port Pin Assignments

The DB-9 serial port on the switch's front panel is used to connect to the switch for out-of-band console configuration. The onboard menu-driven configuration program can be accessed from a terminal or a PC running a terminal emulation program. The pin assignments used to connect to the serial port are provided in the following tables.

Figure 4-4. DB-9 Console Port Pin Numbers



DB-9 Port Pin Assignments

EIA Circuit	CCITT Signal	Description	Switch's DB9 DTE Pin #	PC DB9 DTE Pin #
BB	104	**RxD** (Received Data)	2	2
BA	103	**TxD** (Transmitted Data)	3	3
AB	102	**SGND** (Signal Ground)	5	5

No other pins are used.

Console Port to 9-Pin DTE Port on PC

Switch's 9-Pin Serial Port	Null Modem	PC's 9-Pin DTE Port
2 RXD	<---------TXD ----------	3 TXD
3 TXD	----------RXD ---------->	2 RXD

© 2004 Foundry Networks, Inc.

Switch's 9-Pin Serial Port	Null Modem	PC's 9-Pin DTE Port
5 SGND	----------SGND ----------	5 SGND

No other pins are used.

Console Port to 25-Pin DTE Port on PC

Switch's 9-Pin Serial Port	Null Modem	PC's 25-Pin DTE Port
2 RXD	<---------TXD ----------	2 TXD
3 TXD	----------RXD ---------->	3 RXD
5 SGND	----------SGND ----------	7 SGND

No other pins are used.

© 2004 Foundry Networks, Inc.

Glossary

10BASE-T

IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3, 4, or 5 UTP cable.

100BASE-TX

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 UTP cable.

1000BASE-T

IEEE 802.3ab specification for Gigabit Ethernet over two pairs of Category 5, 5e 100-ohm UTP cable.

1000BASE-X

IEEE 802.3 shorthand term for any 1000 Mbps Gigabit Ethernet based on 8B/10B signaling.

Access Control List (ACL)

ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

Auto-negotiation

Signalling method allowing each node to select its optimum operational mode (e.g., 10, 100, or 1000 Mbps and half or full duplex) based on the capabilities of the node to which it is connected.

Bandwidth

The difference between the highest and lowest frequencies available for network signals. Also synonymous with wire speed, the actual speed of the data transmission along the cable.

BOOTP

Boot protocol used to load the operating system for devices connected to the network.

Collision

A condition in which packets transmitted over the cable interfere with each other. Their interference makes both signals unintelligible.

Collision Domain

Single CSMA/CD LAN segment.

© 2004 Foundry Networks, Inc.

Class of Service (CoS)

CoS is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

CSMA/CD

Carrier Sense Multiple Access/Collision Detect is the communication method employed by Ethernet and Fast Ethernet.

Dynamic Host Control Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Differentiated Services Code Point Service (DSCP)

DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

Extensible Authentication Protocol over LAN (EAPOL)

EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1x Port Authentication standard.

End Station

A workstation, server, or other device that does not act as a network interconnection.

Ethernet

A network communication system developed and standardized by DEC, Intel, and Xerox, using baseband transmission, CSMA/CD access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for integration into the OSI model and extends the physical layer and media with repeaters and implementations that operate on fiber, thin coax and twisted-pair cable.

Fast Ethernet

A 100 Mbps network communication system based on Ethernet and the CSMA/CD access method.

Full Duplex

Transmission method that allows switch and network card to transmit and receive concurrently, effectively doubling the bandwidth of that link.

GARP VLAN Registration Protocol (GVRP)

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the spanning tree so that VLANs defined in each switch can work automatically over a spanning tree network.

 © 2004 Foundry Networks, Inc.

Generic Attribute Registration Protocol (GARP)

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

Generic Multicast Registration Protocol (GMRP)

GMRP allows network devices to register endstations with multicast groups. GMRP requires that any participating network devices or endstations comply with the IEEE 802.1p standard.

Gigabit Ethernet

A 1000 Mbps network communication system based on Ethernet and the CSMA/CD access method.

Group Attribute Registration Protocol

See Generic Attribute Registration Protocol.

IEEE 802.1D

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q

VLAN Tagging – Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p

An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1s

An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

IEEE 802.1x

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3

Defines carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

IEEE 802.3ab

Defines CSMA/CD access method and physical layer specifications for 1000BASE-T Gigabit Ethernet.

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

IEEE 802.3u

Defines CSMA/CD access method and physical layer specifications for 100BASE-TX Fast Ethernet.

 © 2004 Foundry Networks, Inc.

IEEE 802.3x

Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links.

IEEE 802.3z

Defines CSMA/CD access method and physical layer specifications for 1000BASE Gigabit Ethernet.

IGMP Snooping

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IGMP Query

On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

Internet Control Message Protocol (ICMP)

Commonly used to send echo messages (i.e., Ping) for monitoring purposes.

Internet Group Management Protocol (IGMP)

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast router on a given subnetwork, one of the routers is made the “querier” and assumes responsibility for keeping track of group membership.

In-Band Management

Management of the network from a station attached directly to the network.

IP Multicast Filtering

A process whereby this switch can pass multicast traffic along to participating hosts.

IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

Layer 2

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Layer 3

Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

Link Aggregation

See Port Trunk.

Link Aggregation Control Protocol (LACP)

Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

 © 2004 Foundry Networks, Inc.

Media Access Control (MAC)

A portion of the networking protocol that governs access to the transmission medium, facilitating the exchange of data between network nodes.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MD5

An algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

Multicast Switching

A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Out-of-Band Management

Management of the network from a station not attached to the network.

Protected Extensible Authentication Protocol (PEAP)

A protocol proposed by Microsoft, Cisco and RSA Security for securely transporting authentication data, including passwords, over 802.11 wireless networks. Like the competing standard Tunneled Transport Layer Security (TTLS), PEAP makes it possible to authenticate wireless LAN clients without requiring them to have certificates, simplifying the architecture of secure wireless LANs.

Priority

See “Class of Service (CoS)” on page 2.

Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

Per VLAN Spanning Tree (PVST)

Foundry propriety for spanning tree applicable to instances of VLANs.

 © 2004 Foundry Networks, Inc.

Remote Authentication Dial-in User Service (RADIUS)

RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

Rapid Spanning Tree Protocol (RSTP)

RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

Remote Monitoring (RMON)

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Routing Information Protocol (RIP)

The RIP protocol seeks to find the shortest route to another device by minimizing the distance-vector, or hop count, which serves as a rough estimate of transmission cost. RIP-2 is a compatible upgrade to RIP. It adds useful capabilities for subnet routing, authentication, and multicast transmissions.

Secure Shell (SSH)

A secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

Simple Mail Transfer Protocol (SMTP)

A standard host-to-host mail transport protocol that operates over TCP, port 25.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Serial Line Internet Protocol (SLIP)

Serial Line Internet Protocol is a standard protocol for point-to-point connections using serial lines.

Spanning Tree Protocol (STP)

A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

Terminal Access Controller Access Control System Plus (TACACS+)

TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

Telnet

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

 © 2004 Foundry Networks, Inc.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

© 2004 Foundry Networks, Inc.

Transport Layer Security (TLS)

Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

Tunneled Transport Layer Security (TTLS)

A proposed wireless security protocol, developed by Funk Software and Certicom, that combines network-based certificates with other authentication such as tokens or passwords. Also known as EAP-TTLS.

User Datagram Protocol (UDP)

UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XModem

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

 © 2004 Foundry Networks, Inc.

Index

Numerics

1Q trunk 3-99
802.1x port authentication 3-34, 4-56

A

Access Control List *See* ACL
Access Control Lists *See* ACL
ACL
  configuration guidelines 3-40
  Extended IP 3-41, 4-68, 4-69, 4-71
  MAC 3-41, 4-68, 4-80, 4-81–4-83
  Standard IP 3-41, 4-68, 4-69, 4-70
address table 3-69, 4-121

B

BOOTP 3-11, 4-97
broadcast storm, threshold 3-64, 4-114
Buffer
  Syslog A-7

C

calender set 4-55
Class of Service
  configuring 3-102
  Layer 3/4 mapping 3-106
  port priority 3-102, 4-165
  queue mapping 3-102, 3-103
community string 3-22, 4-91
community VLANs 4-150
configuration settings, saving or restoring 3-13, 4-14
console port pin assignments D-1

D

default priority, ingress port 3-102
default settings 2-9
DHCP 3-11, 4-97
dot1x
  global parameters 3-36, 4-66
  port mode 3-37, 4-63
  statistics 3-38, 4-66
downloading software 3-12, 4-14
DSCP, priority mapping 3-109, 4-170
dynamic addresses, displaying 4-122

E

edge port, STP 3-82, 3-84, 4-135
error message logging 4-37
Event
  Syslog A-2

F

Facility
  Syslog A-7
firmware version, displaying 3-7
firmware, upgrading 3-12, 4-14
flow control, configuration 3-54, 4-112

G

GARP timers, setting 3-98, 4-155
GARP VLAN Registration Protocol *See* GVRP
GVRP 3-91, 3-98, 4-153
GVRP, global setting 3-92

H

hardware version, displaying 3-7
HTTP, secure server 3-27, 4-25
HTTPS 3-27, 4-25

© 2004 Foundry Networks, Inc.

I

IEEE 802.1D 3-72
IEEE 802.1Q 3-91
IEEE 802.1w 3-72
IEEE 802.1x 3-34, 4-56
IGMP snooping 3-115
IGMP, configuring 3-114, 4-157
ingress filtering 3-99
IP address
  BOOTP/DHCP service 3-11, 4-97
  setting 3-10, 4-97
IP DSCP mapping 3-109, 4-170
IP port mapping 3-110, 4-172
IP precedence mapping 3-107, 4-169

J

jumbo frames, configuring 4-23

L

LACP 4-178
link aggregation 3-56, 4-177
link type, STP 3-81, 4-136
logging
  configuring 4-38
  enabling 4-37
  syslog traps 4-40
  to syslog servers 4-39
log-in
  CLI 4-1
  Web interface 3-2
logon authentication
  RADIUS server 3-25
  TACACS server 3-25, 4-61
logon authentication, sequence 4-58

M

main menu 3-3
mirror port, configuring 3-66
MSTP
  global settings 4-124
  interface settings 4-124
multicast
  configuring 3-114, 4-157
  IGMP query 3-115
  IGMP snooping 3-115
  registration table 3-118, 4-160
  router 3-116, 4-163

P

passwords
  administrator setting 3-24
  support 1-1
path cost method 3-79, 4-128
path cost, STP 4-133
pin assignments
  25-pin DTE port D-2
  9-pin DTE port D-1
  console port D-1
port authentication 3-34, 4-56
port configuration
  autonegotiation 3-54, 4-110
  capabilities 3-54, 4-111
  displaying 3-52
  flow control 3-54, 4-112
port priority
  configuring 3-102, 4-165
  default ingress 3-102
port security, configuring 3-32, 4-114
priority
  default port ingress 3-102
  IP DSCP 3-109, 4-170
  IP port 3-110, 4-172
  IP precedence 3-107, 4-169
  Layer 3/4 mapping 3-106
priority, STP 3-78, 4-127
private VLANs, configuring 4-149
problems, troubleshooting B-1
prompt, configuring for CLI 4-12
protocol migration 3-84, 4-136

Q

querier, IGMP snooping 3-115, 4-160

R

RADIUS 3-25, 4-56
rate limits, setting 3-67, 4-186
remote logging 4-40
RSTP, global configuration 3-77

S

secure shell 4-27
Secure Shell configuration 4-29, 4-30, 4-35
Secure Socket Layer *See* SSL
serial port, configuring 4-101
show marker 4-55
SNMP
  community string 3-22, 4-91
  enabling traps 3-23, 4-94
  filtering IP addresses 3-51
  Syslog A-2
  trap manager 3-23, 4-93
snooping, IGMP 3-115
software downloads 3-12, 4-14
software version, displaying 3-7
Spanning Tree Protocol 3-72, 3-90, 4-124
Spanning Tree Type 3-78
SSH, configuring 4-29, 4-30, 4-35
SSL 4-25

 © 2004 Foundry Networks, Inc.

STA
  interface settings 3-87, 3-89
startup files
  displaying 3-12, 4-16
  setting 3-12, 4-17
statistics, switch 3-120, 4-118
STP 4-124, 4-125
  configuring interfaces 3-83, 4-124
  edge port 3-82, 3-84, 4-135
  interface settings 3-81, 4-139
  link type 3-81, 4-136
  path cost 3-82, 3-84, 4-128
  path cost method 3-79
  priority 3-78, 4-127, 4-134
  protocol migration 3-84, 4-136
support, technical 1-1
Syslog A-2
  buffer A-7
  changing facility A-7
  server A-6
system clock, setting 3-20, 4-51
System Logs 3-15
system software, downloading from server 3-12, 4-14

T

TACACS 3-25, 4-56
tagged frames, VLAN 3-90
technical support 1-1
  e-mail 1-1
  telephone 1-2
  Web 1-1
time, setting 3-20, 4-51
Trap
  Syslog A-2
trap manager 3-23, 4-93
troubleshooting B-1
trunk
  configuration 3-56, 4-177
  static 3-55

U

unit ID, displaying 4-24
untagged VLANs 3-91
upgrading software 3-12, 4-14, C-1
user password 3-24

V

VLANs
  adding interfaces 3-96, 3-98, 4-147
  creating 3-95
  current table 3-93
  forbidden 3-97, 4-148
  ingress filtering 4-145
  interface configuration 3-98
  PVID 4-146

W

Web interface
  access requirements 3-1
  configuration buttons 3-2
  home page 3-2
  menu list 3-3
  panel display 3-3

 © 2004 Foundry Networks, Inc.

 © 2004 Foundry Networks, Inc.